Xarxes socials: vigilància i control a través de les noves tecnologies en un món global

Carles Rodríguez González

NIU: 1499073

Juny de 2020

Treball Final de Grau

Humanitats

Curs 2019 – 2020

Tutor: Miquel Solana Solana

Universitat Autònoma de Barcelona

Resum:

Les xarxes socials s'han convertit en el principal espai de comunicació de la societat en un món globalitzat com l'actual. L'espectacular utilització dels dispositius mòbils com els telèfons intel·ligents que habitualment portem sempre amb nosaltres, ha facilitat el fet de poder interactuar, buscar informació o consultar notícies des de qualsevol lloc i en tot moment. Això ha creat una certa addicció i dependència al sistema. Per una altra banda, les elits de poder i les gran corporacions del món de la comunicació, han vist la manera d'incrementar els seus beneficis tenint sota control els usuaris. Les tecnologies de la informació i la comunicació han desenvolupat programes algorítmics per aconseguir el màxim nombre de dades de la població seguint els seus hàbits i comportament. El *big data* es consolida com un dels objectius d'aquestes empreses. Avui dia tot el que fem genera dades i aquestes dades poden tenir un valor incalculable per a moltes finalitats. La tecnologia ha propiciat la creació d'importants programes de vigilància per part de les agències de seguretat de molts països. Les principals empreses del món de la comunicació com Google o Facebook ens proporcionen serveis a canvi que nosaltres facilitem les nostres dades, i a través d'aquí van elaborant uns perfils que cada vegada són més complets. Sense cap dubte es pot afirmar que estem sent vigilats i espiats de manera permanent.

Paraules clau: Algoritme, big data, control, internet, vigilància, xarxa social.

Resumen:

Las redes sociales se han convertido en el principal medio de comunicación de la sociedad en un mundo globalizado cómo el actual. La espectacular utilización de los dispositivos móviles como los teléfonos inteligentes que habitualmente llevamos siempre con nosotros, ha facilitado la manera de poder interactuar, buscar información o consultar noticias desde cualquier lugar y en todo momento. Esto ha generado una cierta adicción y dependencia del sistema. Por otro lado, las élites de poder y las grandes corporaciones del mundo de la comunicación, han visto la manera de incrementar sus beneficios teniendo bajo control a los usuarios. Las tecnologías de la información y la comunicación han desarrollado programas algorítmicos para conseguir la máxima cantidad de datos de la población, seguir sus hábitos y comportamiento. El *big data* se consolida como uno de los objetivos de estas empresas. Hoy día todo lo que hacemos en la red genera datos y éstos, pueden llegar a tener un valor incalculable para distintas finalidades. La tecnología ha propiciado la creación de importantes programas de vigilancia a través de las agencias de seguridad de distintos países. Las principales empresas del mundo de la comunicación como Google o Facebook nos proporcionan servicios a cambio de que nosotros facilitemos nuestros datos y a través de éstos van elaborando unos perfiles que cada vez son más completos. Sin ninguna duda, se puede afirmar que estamos siendo vigilados y espiados de manera permanente.

Palabras clave: Algoritmo, big data, control, internet, red social, vigilancia.

Abstract:

The social networks have become society's main venue of communication in the current globalized world. The spectacular use of mobile devices such as smart phones that we carry all the time has facilitated being able to interact, search information or check up the news from anywhere and anytime. This has created a certain addiction and dependency to the system. On the other hand, the power elites and the big corporations of the media world, have seen a way to increment their profits while having the users under their control. The information and communication technologies have developed algorithmic programs to gather the maximum amount possible of data on the population following their habits and behavior. Big Data has become one of the main goals of these companies. Nowadays everything we do generates data and this data can have an incalculable value for many ends. Technology has facilitated the creation of important surveillance programs by security agencies of many countries. The main companies from the communication world, such as Google or Facebook offer us services in exchange for our data, and from here they elaborate profiles continually under growth. Without a doubt it can be said that we are under surveillance and spied upon permanently.

Key words: Algorithm, big data, control, internet, vigilance, social network.

Índex

1. Introducció

En els primers anys del segle XXI s'han produït diversos canvis en l'àmbit de la comunicació que han posat en relleu com a través de les noves tecnologies s'ha generat una nova manera d'interactuar, en la que l'individu es lliura de manera voluntària a la pèrdua de privacitat, facilitant tot tipus d'informació i dades personals, no sent conscient de les conseqüències que això representa.

L'espectacular creixement de les xarxes socials, com si d'una teranyina es tractés, ha anat atrapant a la majora de la població. Primer va ser com a novetat i després com una part d'integració dels individus dintre de la societat, on no para de guanyar adeptes. Aquest fet sembla confirmar que gairebé és obligatori estar a dins aquest sistema de comunicació social i global per evitar una certa exclusió dels nostres propis grups de relació en l'àmbit de les noves tecnologies.

Avui dia sembla que cada vegada es parla menys i que gairebé tot es diu a través de les xarxes socials. Des d'un punt de vista neutre, la reflexió és obligada: cap a on anem? Realment estem protegits cada vegada que cliquem un "accepto"? És bo aquest excés de comunicació social telemàtica? La societat de la informació està encaminada cap el control total per part de les elits de poder?

La utilització del telèfon mòbil ens està afectant de manera considerable en la vida quotidiana, només cal observar pel carrer i veure que cada vegada més gent està consultant dades, llegint les noticies, escrivint missatges o compartint coses a les xarxes socials. També es veu al tren, a l'autobús i al metro, i es fàcil observar que la majoria de les persones tenen entre les seves mans un d'aquests aparells. Amb això es veu aquesta necessitat d'estar connectats i d'intercanviar informació el més aviat possible.

Les noves tecnologies estan avançant tant ràpid que pràcticament ho abasten tot. Sorgeixen aplicacions sense parar però no solament són protagonistes els nostres dispositius mòbils i ordinadors personals. Contínuament es creen programes i aplicacions per a qualsevol cosa. La publicitat i la monetització cada vegada està sent més present, l'objectiu és atrapar a la població i mantenir-la sota control dintre del sistema.

Aquest estat de vigilància i control ha estat decisiu principalment a dos elements:

- Internet

- Els dispositius mòbils com els telèfons intel·ligents i que habitualment portem sempre amb nosaltres, delatant on som i que fem.

Per una altra banda, *algoritme*, *big data* i *bot*, són tres definicions fonamentals sense les quals el «sistema» no pot funcionar. En cada apartat es veurà quina és cadascuna d'aquestes i la incidència que tenen en la vida quotidiana.

L'estructura del treball està formada per un tema principal i a més a més té quatre subapartats per tal de tractar cada part de manera més precisa. De totes formes, el tema central: les *xarxes socials* i el subapartat *vigilància i control* són els més extensos a causa del contingut, les dades i els gràfics que s'hi incorporen. També s'ha cregut oportú citar els noms d'algunes empreses, programes i exemples de les eines utilitzades en les tecnologies de la informació i comunicació per mostrar com funcionen i quina incidència tenen.

2. Objectius

Objectius generals

L'objectiu d'aquest treball és mostrar amb evidencies i arguments, que en els últims anys les agències de seguretat d'alguns governs, les grans corporacions i les empreses del món de la comunicació, han creat unes estructures a escala global que tenen com a finalitat el control social de la població amb la utilització de diverses eines desenvolupades en el camp de les noves tecnologies.

¿I perquè es vol aquest control social de la població?

Hi ha moltes referències als sofisticats mètodes, que utilitzen cada vegada més aquestes empreses, per influenciar a la població, amb finalitats publicitàries i econòmiques, envaint la privacitat per arribar a cada usuari de manera personalitzada. El motiu, és oferir els seus productes gràcies als perfils que han anat elaborant a través de les nostres consultes i recerques, que no han parat de créixer a la xarxa.

Els complexos algoritmes creats per matemàtics i programadors de les grans empreses de Silicon Valley com Google, Facebook i altres, s'encarreguen de fer que tot això sigui possible. El seus objectius sense cap dubte són saber cada vegada més coses dels usuaris, establint uns criteris de control en els quals, nosaltres som el producte.

Caldrà indagar per tal de posar al descobert moltes de les coses que evidencien els mètodes que fan servir per vigilar, controlar i manipular els hàbits de la població.

Objectius específics

- Com va començar tot: una breu història d'internet.

Per tenir un punt de referencia, es molt important situar-se el els orígens per saber com va néixer internet, empreses, agències i tot el desenvolupament tecnològic posterior, que culmina amb la implantació de les xarxes socials a escala global.

- Les xarxes socials.

Què és una xarxa social? com funciona i com està estructurada? Què hi ha al darrera una xarxa social?

- Vigilància i control.

Tècniques i maneres utilitzades per les agències de seguretat d'alguns governs i empreses del món de les tecnologies de la informació i comunicació.

- Què són els algoritmes?

Cada vegada se sent a parlar més de l'expressió *algoritme*, però realment, cal explicar què és, què fa, i quina és la seva funció.

- Què és el big data? Quines finalitats té?

En els darrers anys l'expressió de *big data* cada vegada té més presència en la vida de les persones.

- Què són els *bots*? Com treballen?

Els bots són elements fonamentals en el camp de les aplicacions que tenen a veure amb les tecnologies a la xarxa.

3. Metodologia

En l'actualitat el volum d'informació es molt gran a causa del creixement en l'ús de les noves tecnologies, i que ja forma part del nostre dia a dia. Per tant, en aquest cas, hi ha tres fonts primordials:

- El material bibliogràfic editat a través de llibres de diversos autors ben reconeguts i especialitzats que amb un cert prestigi han abordat aquests temes, i que provenen dels camps de la sociologia, la filosofia, la història o de la tecnologia.
- Un altre mitjà no menys important és internet, que en els darrers anys s'ha anat nodrint gairebé de tots els esdeveniments que han passat al món, a dia d'avui s'ha convertit en una font de consulta molt important perquè durant els darrers anys s'ha consolidat com a lloc de referència de la informació digital. A part, a la xarxa també s'hi troben treballs, documentals, estudis i publicacions.
- La premsa diària és una altre font d'informació destacable on apareixen moltes de les noticies relacionades amb les últimes investigacions i esdeveniments recents.

Els autors i autores seleccionats en la part de bibliografia, tracten de manera destacada molts aspectes que són utilitzats en el tema central d'aquest treball. A través d'aquests investigadors, es pot arribar a conèixer com ens afecta la utilització de les eines informàtiques i de comunicació en la vida quotidiana, des dels ordinadors personals als telèfons intel·ligents o smartphones.

Aquests autors són: el filòsof *Byung-Chul Han,* l'historiador *Yuval Noah Harari, la matemàtica Cathy O'Neil,* la catedràtica de la University of California-Santa Barbara *Dawn E. Holmes,* les celebritats de Silicon Valley *Eli Parisier i Jaron Lanier*, per citar-ne només alguns. Per una altre banda també és de destacar Edward Snowden, qui relata en primera persona i com ex-analista, els mètodes d'actuar de la NSA (Agencia de Seguretat dels Estat Units) sobre l'espionatge i control de la població mitjançant els dispositius de comunicació.

Fer una tria i contrastar aquestes informacions, ha estat un dels punts per la elaboració del treball.

La recerca a les biblioteques, escollir els temes, autors, llibres, documentals i articles d'internet ha estat una feina molt àrdua i selectiva per tal d'acollir-se als objectius i l'extensió requerida.

També es pot dir que en aquest cas, la tecnologia ha facilitat l'accés a una bona part d'informació. Però el punt de partida de cada tema principalment ha estat des dels llibres seleccionats on la informació i dades, tenen els dos elements bàsics: *qualitat i fiabilitat*.

La temàtica en general, dóna per molt i en els darrers temps estan apareixent moltes noticies en els mitjans de comunicació, tant a la premsa com a la televisió, però l'objectiu era trobar uns punts centrals on justificar i desenvolupar el treball.

4. Les xarxes socials

El gran entramat construït per les agencies de seguretat i les grans empreses del món de la comunicació ha estat possible a causa de la creació i evolució de la tecnologia informàtica en la qual hi han participat matemàtics, científics i militars.

Inicialment es tractava d'una qüestió de defensa però amb el pas del temps i les millores tècniques, van anar apareixen altres camps d'aplicació. Ara es pot observar que el fet principal és incidir en la vida quotidiana de la societat, sent l'individu l'objecte principal.

L'origen d'internet és remunta al 1958 quan neix l'agència governamental de seguretat dels Estats Units A.R.P.A. (Advanced Research Projects Agency) creada per respondre als desafiaments militars i tecnològics de la Unió Soviètica (URSS). A la següent cronologia es fan constar només algunes dates i fets rellevants amb la finalitat d'adequar-ho al tema central del projecte. (Figura 1)

Figura 1 (Taula cronològica)

ANY	DESCRIPCIÓ	AUTOR/S
1969	Creació d'ARPANET (Advanced Research Projects Agency Network). L'objectiu era establir una xarxa com a mitjà de comunicació per a diferents organismes del país. Bàsicament es tractava d'una xarxa informàtica on el node central estava a la mateixa Universitat de Califòrnia.	Universitat de Califòrnia i el Departament de Defensa dels EUA.
1972	Es fa la primera demostració pública d'ARPANET enviant un missatge de l'oest a l'est dels Estats Units.	Universitat de Califòrnia i el Departament de Defensa dels EUA.
1987	El número de HOST (computadora o un altre dispositiu connectat a una xarxa informàtica) a internet ja són més de 10.000 i això va ser una de les premonicions del que serà la interconnexió humana a escala global generada per mitjans electrònics.	
1987	Creació del DNS (Domain Name System), el sistema de noms que faria possible crear els dominis d'internet.	Paul Mockapetris
1989	Internet creix de forma descomunal. Hi ha 50.000 xarxes, 4 milions de sistemes, 70 milions d'usuaris. Internet comença a tenir ús comercial.	
1991	Es crea la WWW (World Wide Web) des del CERN (Conseil Européen pour la Recherche Nucléaire) utilitzant el llenguatge d'hipertext. De fet, el CERN és conegut actualment com a *Laboratori Europeu de Física de partícules*.	CERN (Conseil Européen pour la Recherche Nucléaire)

1993	Creació de *Mosaic*, un programa que permetia navegar per internet amb major facilitat. Després es convertiria en *Netscape*. Va ser el començament dels navegadors.	Marc Andressen
1994	Creació d'Amazon, la botiga més gran del món en venda de llibres.	Jeff Bezos
	Es crea Yahoo! Un altre dels navegadors importants.	Jerry Yang i David Filo
1995	Neixen els blogs	Justin Hall
	Es crea a Califòrnia eBay, el primer lloc de subhastes a internet.	Pierre Omidyar
1998	Creació de Google.	Larry Page i Sergei Brin
2001	Es crea Wikipèdia. La més gran i popular enciclopèdia d'internet.	Jimmy Wales i Larry Sanger
2002	Creació de la primera xarxa social del món: Myespace	Jonathan Abrams
2004	Creació de Facebook	Mark Zuckerberg
	Es crea Youtube	Chad Harley, Steve Chen i Jawed Karim
2005	A Youtube es visualitzen més de 100 milions de vídeos al dia.	Chad Harley, Steve Chen i Jawed Karim
2006	Internet arriba als 1.100 milions d'usuaris.	
	Es posa en marxa Twitter.	Jack Dorsey
	Google adquireix Youtube per un valor de 1.650 milions de dòlars.	
2007	Amazon crea el lector de llibres Kindle.	
	Apareix l'IPhone, primer dispositiu mòbil multimèdia amb connexió a internet. A partir d'aquí una gran part del tràfic d'internet és a través dels dispositius mòbils.	Apple
2008	Es calcula que hi ha 63.000 milions de pàgines web	
2009	Creació de WhatsApp	Brian Acton i Jan Koum
2010	Hi ha 1.966 milions d'usuaris a internet	
	Creació d'Instagram	Kevin Systrom i Mike Krieger
2011	Facebook arriba als 600 milions d'usuaris	
2012	Facebook adquireix Instagram per 1.000 milions de dòlars.[1]	
2014	Facebook Inc. adquireix WhatsApp per 19.000 milions de dòlars.[2] Tenia 450 milions d'usuaris	
2019	Internet arriba als 4.388 milions d'usuaris	

Font: https://es.wikipedia.org/wiki/Historia_de_Internet (Consultat: 21/01/2020)

Font: https://www.youtube.com/watch?v=i4RE6dBAjH4&t=44s (Consultat: 21/01/2020)

Amb aquest resum històric és pretén relacionar la gradual creació d'empreses tecnològiques de la comunicació amb el creixement d'usuaris. Si bé, a finals dels anys vuitanta del segle XX era quan es començava a conèixer internet, no va ser fins a mitjans de la dècada de 1990 quan va anar creixent pel tot el món, tot i que no hi havia una estimació de l'efecte que això arribaria a tenir. Si observem, es veu clarament el creixement exponencial d'usuaris d'internet, on actualment més de la

[1] http://tublogtecnologico.com/instagram-la-red-social-que-mas-crece/ (Consultat: 21/01/2020)

[2] https://www.expansion.com/2014/02/19/empresas/tmt/1392849185.html (Consultat: 21/01/2020)

meitat de la població del planeta ja disposa d'accés a la xarxa, i això, inclou tant els països avançats com els menys desenvolupats. Aquest fet consolida internet com l'eina de comunicació global i amb aquesta la necessitat de formar part de les xarxes socials.

Les elits de poder, els governs i les grans corporacions són conscients d'aquesta dependència de la població a les xarxes socials, per tant, es pot parlar de la elaboració d'un complex pla que les eines tecnològiques han proporcionat perquè cada individu pugui fer-ne ús a tots els nivells, des de comunicar-se amb el seu cercle d'amistats o els de l'àmbit laboral, realitzar gestions administratives, fiscals, sanitàries, docents, d'oci, culturals i compres, com per exemple pot arribar a ser la planificació i despeses d'un viatge.

Amb tot el ventall de possibilitats, resulta ben fàcil que des d'aquestes empreses i a canvi d'utilitzar les seves plataformes, lliurem importants dades personals que després podran utilitzar per vendre-les a tercers, i obtenir importants ingressos econòmics.

Un gran sector de la població, en especial en una franja d'edat jove i que correspon amb els anomenats *Millennials*[3] és qui participa i en fa més ús de les xarxes socials. Actualment és habitual posar qualsevol tipus d'informació i dades a la xarxa on les pot veure gairebé tothom, des de textos fins a fotografies o vídeos, tot i que en alguns casos es pugui restringir l'accés, el que està clar es que tota la informació que es lliura a la xarxa, ja queda allà, és a dir en els «núvols» o servidors centrals de cada empresa, res no es perd, i allà anirà creixent per sempre. Aquesta capacitat de fer a la gent addicta, a base d'estímuls, fa que cada vegada s'incrementi més el nombre d'usuaris.

Aquestes mateixes empreses competeixen entre elles per atraure el major nombre d'usuaris, que en realitat seran «clients», perquè una de les raons principals, també és de fons econòmic.

Tenir les dades per saber-ho tot de cada individu, però també per quan convé, poder vendre-les a terceres empreses per finalitats econòmiques, publicitàries i comercials.

Hi ha una infinitat de xarxes socials a tot el món, però és ben conegut quines són les que lideren el «mercat». Sense dubte Facebook porta uns anys al capdavant, però cal afegir les altres empreses que han adquirit, per tant, això representa una xifra realment preocupant perquè un sol grup empresarial (Facebook, WhatsApp, Instagram) aglutina la majoria de la població, a prop de 5.000 milions d'usuaris només amb aquestes tres empreses.

Sabem, però que alguns d'aquests usuaris poden estar en dues d'aquestes companyies, però tot i així parlem d'una significativa xifra d'individus.

Cal destacar que un canal per visualitzar vídeos com Youtube (que és propietat de Google) entra també dins d'aquesta categoria, amb 2.000 milions d'usuaris.

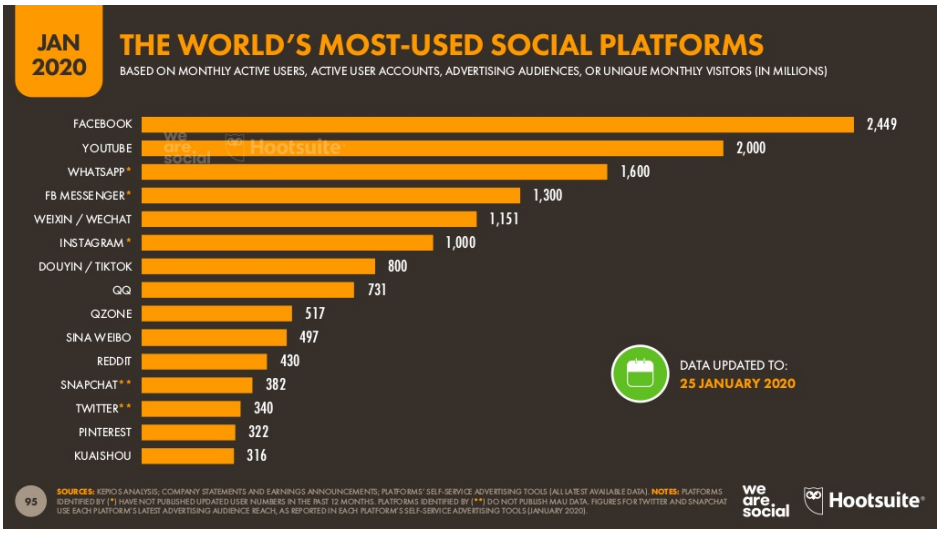
A part, caldria mencionar que a la Xina, i a causa de temes de censura i restriccions polítiques, disposen de xarxes úniques per l'ús intern i exclusiu de la pròpia població,

[3] http://tublogtecnologico.com/las-redes-sociales-mas-utilizadas-segun-la-edad/ (nascuts entre 1980 i 1995)

tot i sent el país més poblat del planeta, junt amb la Índia, estan per sota de la suma de les xarxes globals, però això, no vol dir que tingui pocs usuaris perquè segons les dades, la xarxa social xinesa Weixin/WeChat supera els 1.100 milions d'usuaris. (Galeano, 2020)

Distribució de les principals xarxes socials on destaca Facebook sobrepassant els 2.400 milions d'usuaris, seguida a prop de Youtube. (Figura 2).

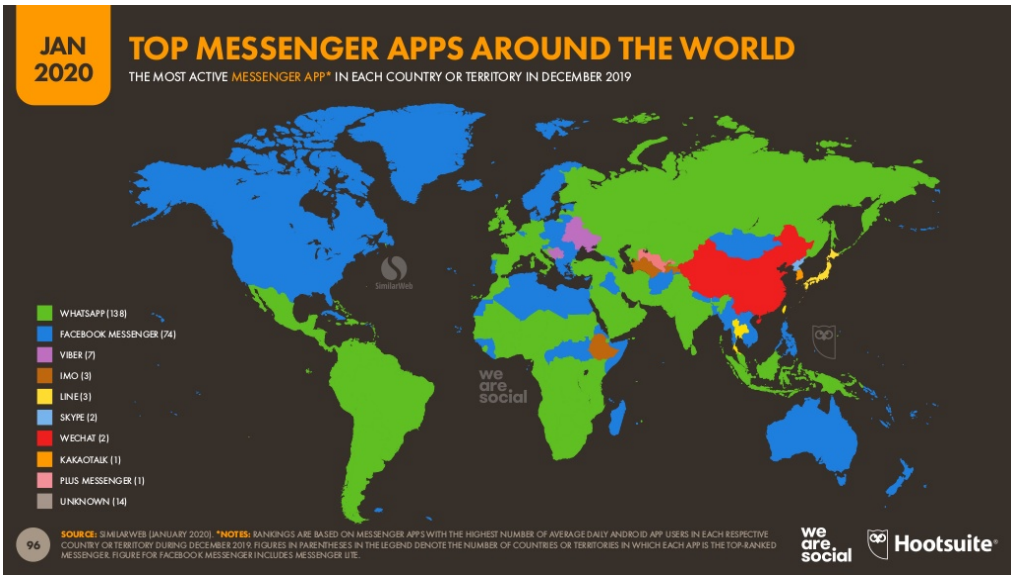
Figura 2 (Gràfic del Ranking d'usuaris)



Font: Galeano (2020): https://marketing4ecommerce.net/cuales-redes-sociales-con-mas-usuarios-mundo-2019-top/ (Consultat: 21/02/2020)

Distribució geogràfica de les xarxes socials de missatgeria (Figura 3) on es mostra per zones a nivell global

Figura 3 (empreses de missatgeria social)



Font: Galeano (2020): https://marketing4ecommerce.net/cuales-redes-sociales-con-mas-usuarios-mundo-2019-top/ (Consultat: 21/02/2020)

En aquests indicadors, no apareix l'altre gran monstre tecnològic com és Google. A efectes oficials Google es considera un navegador, o motor de cerca, però en el fons també es tracte d'un sistema, el qual disposa d'un ventall d'eines que acaba sent també una «màquina de controlar i espiar» de la mateixa manera que ho fa una xarxa social com Facebook.

De fet, Facebook i Google són les dues empreses que amb les seves estratègies, s'han fet amb la majoria d'usuaris.

De totes formes, oficialment Google i els seus serveis estan registrats i dins d'un conglomerat d'empreses sota el nom d' *Alphabet*[4], que és amb el qual cotitza a la borsa. (Lanier, 2018: 159-160)

Google com a navegador és líder mundial i el preferit per la majoria de la població per realitzar cerques, buscar informació i fer tràmits a través d'internet, però mostra una gran opacitat, dóna molts serveis a l'usuari en tot el seu conjunt d'aplicacions, però a canvi que aquest faciliti moltes dades personals.

> Uno de los principios fundamentales en los que se basa Google es que debemos respetar a los usuarios en todo lo que hacemos. A medida que evoluciona Internet, eso implica mejorar continuamente nuestras tecnologías de seguridad y herramientas de privacidad para que los usuarios y sus familias estén seguros online.
>
> (un dels eslògans de Google)

Per una altra banda va animant a l'usuari a participar en les tasques que fa per tal de fixar un seguit de referencies :

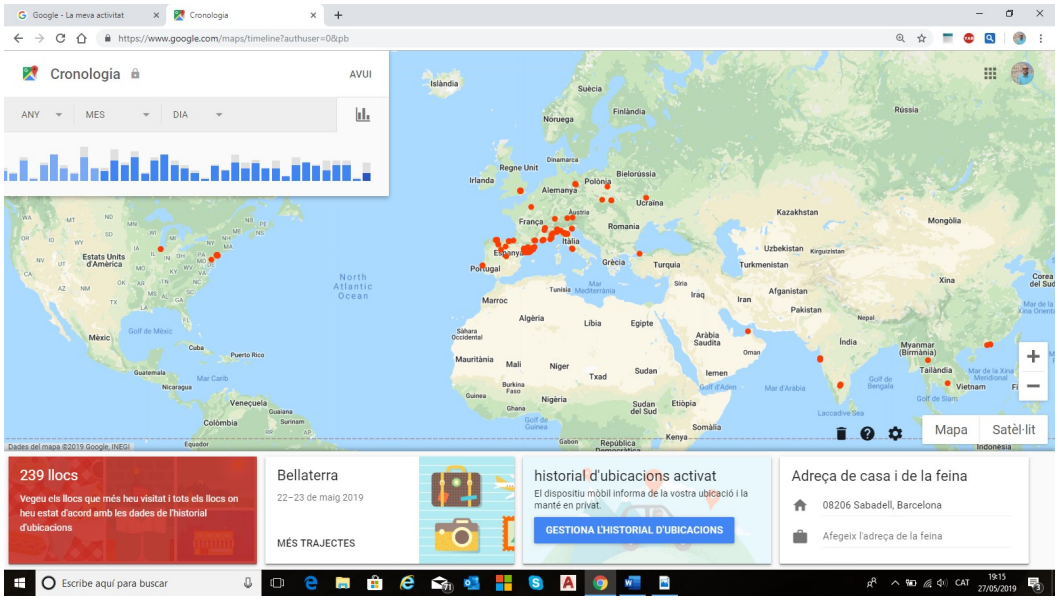
> Guarda tu actividad en los sitios web y las aplicaciones de Google (incluida la información asociada, como la ubicación) para ofrecerte búsquedas más rápidas, mejores recomendaciones y experiencias más personalizadas en Maps, la Búsqueda y otros servicios de Google.
>
> (informació del compte de Google)

Es veu com de manera encoberta s'aparenta que volen ajudar a personalitzar les necessitats de l'usuari amb l'excusa de «recerques més ràpides» i «millors recomanacions». Per exemple, perquè volen saber la ubicació? Com es veurà, tot queda guardat en el perfil de cada persona. Les activitats d'un usuari quan porta el dispositiu a sobre, es poden trobar al compte de Google / Cronologia.

Un fet per demostrar la informació i dades que poden tenir d'un usuari, es que fins i tot, en un mapa arriben a sortir marcats amb tota classe de dades (coordenades, imatges i altres informacions), els llocs del món (Figura 4) on ha estat al llarg de la vida portant els dispositius mòbils a sobre.

[4] https://ca.wikipedia.org/wiki/Alphabet_Inc. (Consulta: 02/02/2020)

Figura 4 (cronologia d'un historial d'ubicacions)



(Imatge: Carles Rodríguez)

Amb tot el que s'ha anat mostrant, no es pot negar que efectivament estem molt més controlats del que podem imaginar, és preocupant veure el que ja hi ha i com això, amb el temps es pot anar incrementant de manera contínua. Encara que a partir d'aquest moment es vulguin modificar o eliminar coses, el fet és que aquestes dades ja les tenen guardades en els seus servidors.

Estem utilitzant els dispositius mòbils contínuament, i la sensació es que ho fem de manera gratuïta, però el cert és que no és així: «Se olvida con mucha facilidad que gratis, significa inevitablemente que otra persona decidirá como vivimos». (Lanier, 2019: 46)

Una de les altres coses a tenir en compte es que habitualment moltes de les dades que es reben o consulten, per no ocupar espai del dispositiu personal, es posen al núvol.

Des del punt de vista d'un usuari normal, un núvol no és res més que un mecanisme d'emmagatzement que garanteix que les dades es processen o emmagatzemen en una sèrie de servidors diferents, en última instància, són propietat de diferents empreses. Com a resultat, aquestes dades realment ja no són de l'usuari. Estan controlades per les empreses[5], qui les podran utilitzar en gairebé qualsevol finalitat. (Snowden, 2019: 264)

Un fet que evidencia el creixement de l'accés a internet es pot observar fàcilment cada dia i pràcticament en tots els llocs. Es especial en els espais públics i el transport (Figura 5). Cada vegada resulta més estrany veure persones que no estiguin consultant el dispositiu mòbil, i aquest per comoditat, s'ha consolidat com a líder d'utilització.

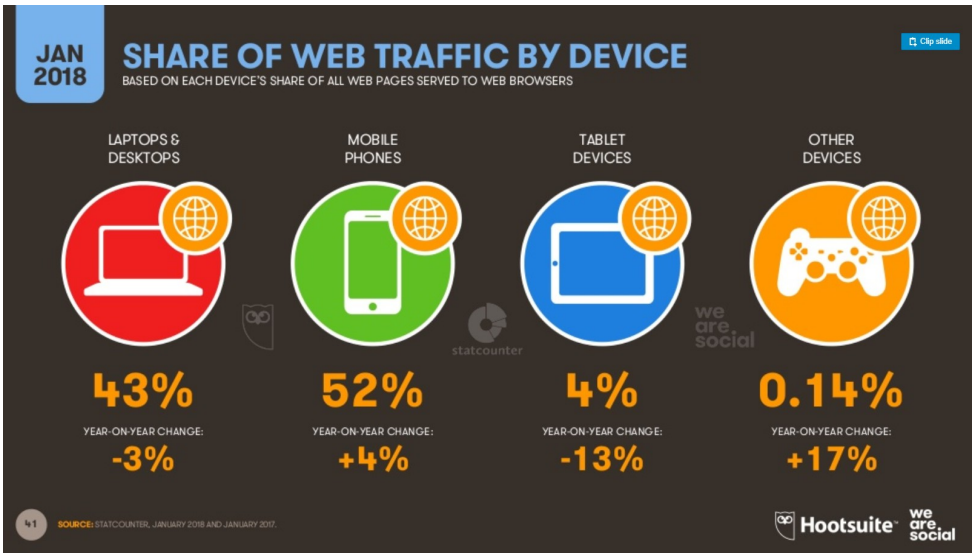
[5] Sempre és recomanable llegir els contractes de privacitat, que per cert, solen tenir més de 6.000 paraules. Quan escollim emmagatzemar dades online al núvol, cedim el nostre dret a reclamar la seva propietat. (Snowden, 2019: 264)

Figura 5 (la majoria d'usuaris connectats a la xarxa)

La majoria d'usuaris consultant els telèfons mòbils. Un dia al matí (17/02/2020) en l'estació Creu Alta de Sabadell dels Ferrocarrils de la Generalitat (Imatge: Carles Rodríguez)

El següent gràfic (Figura 6) permet mostrar com efectivament els telèfons mòbils s'han convertit en l'eina més utilitzada i que més està creixent, desplaçant d'aquesta manera als ordinadors i tablets.

Figura 6 (percentatges de creixement segons el dispositiu)



Galeano (2020): https://marketing4ecommerce.net/cuales-redes-sociales-con-mas-usuarios-mundo-2019-top/

El gràfic mostra el creixement i domini que es fa d'internet a través dels dispositius mòbils. Això realment és una dada destacable que confirma que si la majoria de la població porta a sobre l'smartphone (telèfon mòbil intel·ligent), facilita encara més l'ús que se'n fa, perquè en aquest cas, es dóna també la ubicació en tot moment i en temps real, cosa que augmenta la precisió dels moviments de l'individu. Aquest 52% confirma que més de la meitat de la població ho fa des d'aquests dispositius mòbils.

Sense dubte que les elits de poder, governs i les grans companyies de les tecnologies de la comunicació ja ho tenen previst i els hi va bé saber cada vegada més coses de nosaltres. Una data important relacionada amb la vigilància massiva.

En els darrers temps se sent a parlar tant en els mitjans de comunicació com entre la població mateixa, de la capacitat que tenen les companyies operadores per espiar, utilitzar les seves dades i saber que fan els seus usuaris. Alguns esdeveniments i noticies que han sortit a la premsa han fet pensar a un sector de la societat plantejant dubtes i generant una certa desconfiança.

El tema de les xarxes socials és tant important per les elits del poder que fins i tot ja són a l'agenda del que es diu que és el grup més poderós del món -*Club Bilderberg*- (https://es.wikipedia.org/wiki/Grupo_Bilderberg) i que reuneix cada any moltes de les persones més influents del planeta que entre altres coses marcaran la política i economia com una manera de control de la població. L'agenda del 2019 i en el punt numero 9 sortia el tema de les xarxes socials tractat com «Las redes sociales como armas[6]».

Està ben clar que el poder de les xarxes socials pot arribar a ser determinant en molts aspectes tenint en compte la capacitat d'actuació i comportament de la població, i també de la informació que se'n pot extreure per diverses finalitats.

Un dels afers crítics referent a les xarxes socials es va produir el 2018 com a conseqüència de l'escàndol de Cambridge Analytica[7] on aquesta consultoria va accedir a més de 50 milions de perfils d'usuaris de Facebook.
En resposta a aquest fet, totes les mirades es van dirigir cap el mateix Mark Zuckerberg qui va assegurar que trobaria la manera d'eliminar l'historial de tothom qui ho volgués. Però just un any després es veu que això no ha estat així:

> Hace un año, tras el escándalo de Cambridge Analytica, Mark Zuckerberg anunció una herramienta para borrar nuestro historial de Facebook. Debe ser dificilísima de desarrollar, porque les ha costado 12 meses, pero parece que ya está aquí. El problema es que aquello de borrar el historial, nada de nada. Lo que hace es desvincular de tu cuenta los datos que empresas de terceros obtienen a través de Facebook, pero no los datos que Facebook ha capturado sobre ti. Y nada se borra.
>
> (Pascual, 2019)

Una vegada més se'ns enganya per fer-nos creure que tot això de les xarxes socials es molt transparent quan veiem que es tot el contrari, la opacitat és el que domina. No renunciaran mai a tota la informació que tenen de nosaltres.

De totes formes el discurs dels magnats de les empreses de les tecnologies de la comunicació només està dirigit a mantenir la bona imatge i per calmar la possible inquietud que els accionistes puguin tenir en moments puntuals quan es produeixin esdeveniments d'aquest tipus i evitar una fugida massiva d'usuaris.

---

[6] https://www.mentealternativa.com/reunion-secreta-club-bilderberg-2019-por-la-supervivencia-del-modelo-parasitario-de-la-banca-liberal/ (publicat: 29/05/2019)

[7] https://es.wikipedia.org/wiki/Cambridge_Analytica#Esc%C3%A1ndalo_de_Facebook (publicat: 17/03/2018)

Però el que si es cert, és que escàndols com aquest fan perdre la desconfiança de la població que cada vegada es més conscient del fet que se'ns vigila i se'ns espia sense que nosaltres ho sapiguem.

Per exemple, a Mark Zuckerberg (Figura 7), en molts actes i conferencies, sovint se li ha vist el seu ordinador portàtil amb un tros de cinta adhesiva tapant la càmera, això ens pot fer pensar que per alguna cosa serà, i que ell mateix coneix perfectament moltes de les tècniques que s'utilitzen per espiar als usuaris activant càmeres i micròfons sense que ells no ho sàpiguen.

Figura 7 (Mark Zuckerberg amb la càmera de l'ordinador tapada)

Font: https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook

(Consultat: 22/11/2019)

Potser un dels perills de la xarxa és la confirmació que les càmeres i micròfons dels nostres dispositius s'activen sense el nostre consentiment i el Mark Zuckerberg ho sap (tal com descriu l'ex analista de la NSA Edward Snowden). De fet quan al 2016 va aparèixer el sistema operatiu Windows 10 ja tenia inclosa de sèrie aquesta particularitat tot i que no es va fer massa publicitat. També caldria dir que hi havia la possibilitat de fer la instal·lació personalitzada per evitar que la càmera es posi en marxa de manera remota cada vegada que el sistema ho decideix.

Quan es parla de xarxes socials la majoria de la gent ho identifica amb Facebook i Twitter, perquè evidentment aquestes dues a part de ser les més utilitzades a tot al món, són purament xarxes socials. De totes formes n'hi ha d'altres menys

anomenades i fins i tot alguna que no està tractada de xarxa social com és el cas de LinkedIn perquè en teoria és d'àmbit professional, Jaron Lanier comenta en aquest cas: «la diferencia radica sencillamente en que sus usuarios tienen algo que hacer más allá de competir con las apariencias sociales (…) Esta red es muy conocida como un sitio dónde impulsar la carrera profesional. Gana dinero principalmente conectando empleadores con posibles empleados, en lugar de hacerlo manipulando personas para que realicen compras o modifiquen su comportamiento en otros aspectos no relacionados con la red» (Lanier, 2018: 69)

En conjunt potser sí que es podria dir això d'aquesta xarxa professional, però en els darrers temps ha caigut una mica en la dinàmica de Facebook o Twitter perquè encara que els seus usuaris mostrin perfils professionals, que poden ser autèntics o no, també es mostra una aparença estètica que busca la imatge i on sovint es fa ús de la missatgeria i de les contribucions, que en certa manera s'aparten de l'àmbit professional en sí, adoptant en certa manera funcions de missatgeria. Possiblement s'hagi contagiat una mica de les altres xarxes socials «pures».

Al documental *Facebookistan*[8] es mostren algunes coses interessants on es posa en relleu la discriminació existent en aquest món digital. Per exemple es pot observar que quan a una xarxa social (en aquest cas Youtube), hi ha alguna cosa que considera que pot afectar la seva imatge, actuen bloquejant l'accés o compte de l'usuari, com és el cas de l'artista i fotògraf danès Peter Øvig que publica les seves obres en les quals s'hi poden veure «nus artístics» realitzats exclusivament com un espai i intenció creativa de l'artista, però en canvi la plataforma social en qüestió reacciona actuant de manera autoritària per qüestions d'imatge, i potser sota pressions perquè ho considera immoral. Un altre cas que surt al documental, és el de Max Schrems (austríac i doctorat en dret) qui després d'estar estudiant les lleis de protecció de dades[9], va presentar una denuncia contra Facebook per les seves polítiques opaques que utilitzen l'espionatge i el control dels seus usuaris en què per exemple, el sol fet de fer una foto, localitza el lloc per les coordenades del seu usuari, fa el seguiment de on ha estat, i també els contactes que ha mantingut amb el seu grup. I com el cas del mateix Schrems, després d'haver eliminat les seves dades al compte de Facebook, mostrava que seguien estant allà.

Aquests són dos clars exemples dels diversos que hi surten, i dels més que hi ha del dia a dia al món de les xarxes socials que evidencien les males pràctiques d'aquestes empreses.

De totes formes la utilització de les xarxes socials té una doble via, perquè si bé, estem sotmesos a una manera de control per les grans empreses, també en fem ús personal o col·lectiu amb altres finalitats. En els darrers anys ja és ben normal que a través de les aplicacions dels nostres smartphones, es facin crides per organitzar esdeveniments i fins i tot accions de molts tipus. Un cas ben clar és el que ha envoltat a Catalunya «el Procés» amb el judici als líders independentistes empresonats. El seguiment dia a dia a les xarxes socials ha estat molt gran, i val a dir, que una vegada que va sortir la «Sentència», diverses aplicacions mòbils han

[8] https://www.youtube.com/watch?v=R7_VuGADn6w

[9] REGLAMENTO DE PROTECCIÓN DE DATOS (UE) 2016 / 679 – Directiva 95/46: https://www.boe.es/doue/2016/119/L00001-00088.pdf

estat l'eina prioritària per convocar concentracions massives i protestes en diversos punts del territori. Es podria dir que gràcies a aquesta nova manera de comunicació s'han fet moltes accions que han quedat dins dels corresponents grups participants i sense que les autoritats poguessin intervenir prèviament. També és cert, que cada persona amb un dispositiu mòbil, sol ser una persona controlada i que elements com el GPS permeten facilitar la seva geolocalització al moment, a part de les imatges, vídeos i trucades que es facin en el lloc en qüestió. També caldria destacar el que en el seu moment es va anomenar *La Primavera Àrab* (Lanier, 2018: 134-136) i en la qual va ser un fet decisiu la participació a les xarxes socials per part de la població a fi d'encapçalar i organitzar aquest moviment per les llibertats d'alguns països del Nord d'Àfrica.
Per norma, les xarxes socials son gratuïtes i l'accés a les mateixes és molt fàcil. Els usuaris es donen d'alta en el lloc, creen el seu propi perfil per a compartir-lo amb altres i deixen que els altres ho vegin. Això inclou informació com el nom de l'usuari, la població on viu, l'historial educatiu i laboral, els seus gustos i fotos. Després l'usuari afegeix "amics" (que realment només són altres usuaris) i els hi dona accés a la informació del seu perfil i els permet comunicar amb altres usuaris a través del lloc compartint informació, fotografies i altres coses. (Giant, 2016: 17-18)

El fenomen de la xarxa social *Facebook* no va tenir precedents, a mida que s'anava escampant semblava que era un mitjà fantàstic per estar en contacte amb la societat. Particulars es donaven d'alta i obrien comptes facilitant tota classe de dades personals sense ser conscients inicialment del que un dia això podria representar. Està clar que *Facebook* semblava un «regal» i entreteniment perfecte on l'usuari es lliurava al medi amb les seves dades i una imatge retocada per mostrar el que no era, però va ser la maquinaria més gran de control social fins a les hores. Mark Zuckerberg ho sabia, potser no al principi, però el fet d'adquirir *WhatsApp* en el seu dia, confirma que aquestes intencions de col·laboració en el control social existeixen de manera evident.

> De la información que dejamos en Internet se dice a veces que es nuestro "tatuaje digital". Todos esos datos quedan vinculados a nosotros para siempre, igual que la tinta permanente. En muchos sentidos, las redes sociales se fundamentan en la confianza.
>
> (Lloyd, 2017: 63)

4.1 Vigilància i control

Edward Snowden[10], analista de l'Agència de Seguretat Nacional (NSA) estava planejant si filtrar o no els documents secrets que demostraven fins a quin punt el govern dels Estats Units desenvolupava un programa de vigilància massiva. Va trobar la inspiració en un documental del 2009 que es deia *«L'home més perillós dels Estats Units: Daniel Ellsberg i els Papers del Pentàgon»*[11]. Quan Snowden va

[10] https://ca.wikipedia.org/wiki/Edward_Snowden

[11] https://www.ccma.cat/tv3/Lhome-mes-perillos-dAmerica-a-Grans-documentals-33/noticia-arxiu/493520/

lliurar el material als periodistes al 2013, Ellsberg va ser un dels primers a donar-li suport públicament i amb això, es van fer amics.

Ellsberg, conegut pel cas Watergate, és un precedent perquè va fer una cosa semblant com Snowden, tot i que entre les dècades de 1960 i de 1970 no hi havia la tecnologia actual, la seva feina va consistir en «*fotocopiar els documents amb una Xerox*» i filtrar una bona part d'aquests a la premsa. En aquests documents es mostrava com el govern dels Estats Units va mentir sobre els esdeveniments relacionats amb la Guerra del Vietnam i moltes operacions militars encobertes com la implicació en l'assassinat del president de Vietnam del Sud al 1963 o l'enviament de milers de soldats amb operacions de bombardeig quan sabien que no eren efectius. Ellsberg cansat que el Pentàgon amagués la veritat, va ser quan va decidir fotocopiar els informes (Dowling, 2010).

Això va causar un gran daltabaix polític i va fer sorgir un moviment pacifista als Estats Units. L'administració de Nixon va quedar al descobert, demandant als mitjans per divulgar secrets oficials, però el Tribunal Suprem, en una decisió històrica els va donar la raó al·legant que era una defensa de la llibertat de premsa, i des d'aquell temps, el govern no pot censurar cap article periodístic:

El 2013 Snowden va fer el mateix que Ellsberg però utilitzant les tecnologies actuals: *«Hi ha documents amb informacions encara més explosives»,* va afirmar Glenn Greenward, columnista del diari britànic *The Guardian* i resident al Brasil, qui va ser el primer en publicar els documents filtrats per Snowden sobre els programes secrets dels Estats Units sobre l'espionatge electrònic. En aquesta reunió que es va fer amb moltes precaucions, Greenward va rebre entre 15.000 i 20.000 documents. (McAskill, 2018)

Tot seguit es pot veure com actuen i els mètodes que utilitzen les agencies de seguretat per espiar als ciutadans, com és el cas de la NSA.

4.1.1 La vigilància massiva de la NSA

A l'estiu del 2013 Edward Snowden va provocar un gran escàndol al filtrar els documents secrets sobre la vigilància del govern dels Estats Units als mitjans de comunicació, aquestes revelacions mostraven com l'Agencia Nacional de Seguretat estava explotant el domini dels Estats Units en els serveis d'internet per a espiar els ciutadans de tot el món. Després de fugir dels Estats Units, i abans d'abandonar Hong Kong (lloc on va fer la entrega dels documents) cap a Rússia, Edward Snowden va comentar al diari xinés *South China Morning Post* que la NSA havia encapçalat més de 61.000 operacions de «hackeig» a nivell mundial, diverses d'aquestes a Hong Kong i Xina continental.

Els objectius a Hong Kong incloïen llocs com la Universitat de Xina, funcionaris públics i empreses. Snowden deia: *«fem un hackeig a les columnes centrals de les xarxes, bàsicament els grans direccionadors – els routers- d'Internet que donen accés a les comunicacions de cents de milers d'ordinadors sense haver de fer-ho en cadascun d'ells».* El govern xinés va manifestar la seva profunda preocupació pels suposats ciberatacs contra els seus ciutadans. Pequin va aprofitar la oportunitat per

a qualificar el govern de Barack Obama d'hipòcrita per crida'ls-hi l'atenció pels seus ciberatacs quan Washington estava fent el mateix (Zaballa, 2017).

Estats Units recull i emmagatzema milers[12] de trucades al dia. Amb tota la informació que la NSA estava recollint dels registres telefònics de desenes de milions de ciutadans va ser com es va conèixer aquest escàndol de l'espionatge i vigilància. El diari britànic *The Guardian* va publicar una ordre secreta d'un tribunal que exigia a l'empresa de telecomunicacions *Verizon* a lliurar totes les dades telefòniques a l'agencia de manera rutinària. (Saiz, 2013)

Verizon i *AT&T*, són dues de les empreses de telefonia més grans del país i estan obligades a facilitar les metadades de totes les trucades que processen, tant nacionals com internacionals en les que al menys un dels usuaris està en el país: «a diario y de forma permanente» (Snowden, 2019: 300). Aquestes metadades inclouen els números telefònics, els números de les targetes de crèdit, els números de sèrie dels telèfons utilitzats, la hora i durada de les trucades. James Clapper, director d'intel·ligència Nacional dels Estats Units va confirmar que el govern havia recollit de manera secreta milions de registres telefònics però va assegurar que es respectaven els drets civils i la privacitat dels ciutadans. De totes formes va advertir que la revelació al públic d'aquests programes havia causat un mal irreversible en la prevenció de futurs atacs terroristes contra els Estats Units, però el principal diari del país, *The Washington Post* va insistir en una editorial que el públic necessitava més explicacions sobre el programa per avaluar si valia la pena per temes de seguretat. (Snowden, 2019)

El programa PRISM

Es un programa de vigilància que es va posar en marxa el 2007 per la NSA i que li permet captar correus electrònics, vídeos, fotografies, missatges de veu, imatges, activitat en les xarxes socials, contrasenyes i altres dades dels usuaris continguts per les principals empreses d'internet dels Estats Units. Les companyies anomenades pels diaris que van publicar detalls del sistema, inclouen a Microsoft i la seva divisió Skype; Google i la seva divisió Youtube; Yahoo; Facebook; AOL; Apple i PalTalk (un servei de xat no tan conegut com els anteriors). Aquestes empreses asseguren que el govern no té un accés directe a les seves grans bases de dades, però si que proveeixen la informació quan el govern la sol·licita. (Snowden, 2019: 300-301)

Gràcies a aquest programa, una vegada un sospitós és identificat, totes les persones amb les que hagi estat en contacte, també seran objecte d'investigació, i al mateix temps, totes les persones que estiguin en les bústies dels correus d'aquestes últimes. No cal dir que molts crítics afirmen que el sistema és una amenaça dels drets humans. Fins el dia 5 d'abril del mateix any 2013 (cas Snowden) ja hi havia 117.675 objectius de vigilància actius en la base de dades PRISM (Márquez, 2013).

[12] https://www.elperiodico.com/es/internacional/20130606/el-espionaje-de-eeuu-recoge-millones-de-llamadas-2410836 (Consultat: 22/11/2019)

El programa TEMPORA

Al Regne Unit hi queda una base secreta que suposadament és el centre d'espionatge més gran del món. Aquesta agència, disposa d'aquest programa anomenat TEMPORA. Els serveis d'Intel·ligència britànics es van veure implicats en l'escàndol de vigilància i espionatge. L'agència britànica d'escoltes electròniques, la *Oficina Central de Comunicació del Govern* (GCHQ[13], per les seves sigles en anglès), va ser acusada de recollir informació d'empreses d'internet a través del sistema PRISM. El diari *The Guardian* va informar que l'agència d'espionatge britànica estava «punxant» cables de fibra òptica que transportaven comunicacions globals i que estaven compartint grans quantitats de dades amb la seva «contrapart» dels Estats Units, la NSA.

Segons l'informe, la GCHQ intervenia 200 cables de fibra òptica, el que li permetia recollir moltes més dades que la agencia americana, cap a uns 600 milions de comunicacions diàries.

Només amb un sol cas, com aquest relat gràcies a les informacions i dades que el mateix Snowden va lliurar a la premsa, es van evidenciar els sistemes d'espionatge de les agències governamentals per sobre de la ciutadania. Podem pensar si això va ser un acte de conciencia o no, però els fets demostren que la societat està sotmesa a una vigilància i control permanent quan utilitza eines informàtiques i de comunicació. (Snowden, 2019)

Periòdicament es van sabent casos perquè apareixen en format de noticies que de vegades passen una mica desapercebudes en els mitjans de comunicació. Altres ens arriben a través de documentals i programes d'investigació. Tot i que cada vegada se'n parla més, la població sembla assumir això como una cosa natural i per norma no fan res per prendre un mínim de precaucions, el «conformisme que mostra la societat» combinat amb les preses d'accedir a la xarxa fa que el sistema no canviï, i les companyies tecnològiques ho saben, el fet innegable es que dediquem moltes hores al dia connectats a internet com també interactuant en les xarxes socials.

En la dècada de 1990, internet encara no havia esta víctima de la història amb aquesta gran injustícia digital protagonitzada per governs i empreses per tal de vincular el màxim possible el personatge *online* d'un usuari, amb la seva identitat jurídica *offline*. (Snowden, 2019: 71). Abans hi havia un anonimat del que fèiem i dèiem a la xarxa quan ens connectàvem a internet, però ara agències i empreses utilitzen les seves eines per tal de identificar els usuaris.

XKEYSCORE[14]

Amb aquesta definició es descriu un sistema informàtic secret i una potent eina que utilitza la l'Agencia de Seguretat Nacional (NSA).

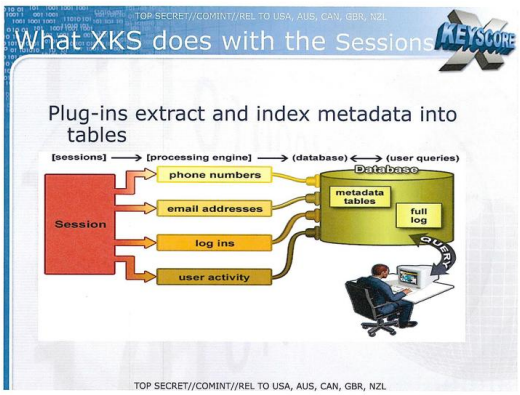
[13] El Film *Secretos de Estado* (2019) descriu un cas basat en fets reals sobre l'espionatge on es mostra com treballa i que és l'agencia d'espionatge britànica GCHQ.

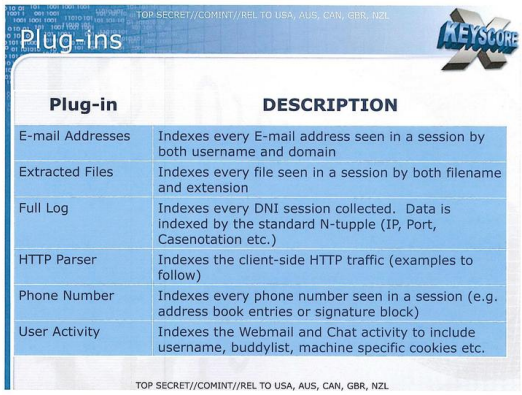
[14] https://es.wikipedia.org/wiki/XKeyscore

En els documents que Edward Snowden va passar als periodistes[15], la NSA descriu XKEYSCORE como la seva «eina de més gran abast», utilitzada per fer cerques en «gairebé tot el que un usuari fa a internet». Les especificacions tècniques expliquen que el sistema va fent «paquets o sessions» i actua fragmentant les dades *online* d'un usuari per fer-les més manejables per la seva anàlisi. Consistia en introduir l'adreça, un número de telèfon o l'adreça IP (numero d'identificació que té cada ordinador) de qualsevol persona, i després bàsicament es tractava de repassar el seu historial de la seva activitat *online*, d'aquesta manera els agents de la NSA veuen la mateixa pantalla i escriptori que la de l'usuari en qüestió. Poden llegir els correus electrònics, les dades de navegació, l'historial de les cerques, les publicacions a les xarxes socials, les fotos i documents que poden haver a l'ordinador, en resum, ho poden veure tot. (Snowden, 2019: 370)

Algunes de les diapositives que formen part d'aquesta presentació de XKEYSCORE (Figura 8) preparada per la formació dels agents de l'Agencia de Seguretat Nacional (NSA).

Figura 8 (imatges d'algunes diapositives de la presentació)





Font: The Guardian (UK) via Edward Snowden via US National Security Agency (NSA)

És important recordar que la NSA també actua en col·laboració amb altres agències de seguretat, a part de l'agència britànica (GCHQ), amb Canadà, Austràlia i Nova Zelanda. Aquests cinc països tenen una aliança que s'anomena FVEY (Five Eyes), els «cinc ulls», però també col·labora amb l'agència de seguretat alemanya (BND). (Snowden, 2019: 433)

Entre els diversos documentals i programes divulgatius que de vegades emeten els diferents canals de televisió, un bon exemple del que hi ha més enllà de les xarxes socials i la vigilància a través d'algunes empreses, seria el de Jordi Basté a TV3 la primavera del 2019 i que va tenir força audiència despertant l'interès de bona part de televidents.

[15] Als periodistes del diari *The Guardian*, Glenn Greenward i Ewen MacAskill, i a la periodista Laura Poitras (directora de documentals com *Citizenfour*), qui les passava a Bart Gellman del Washington Post.

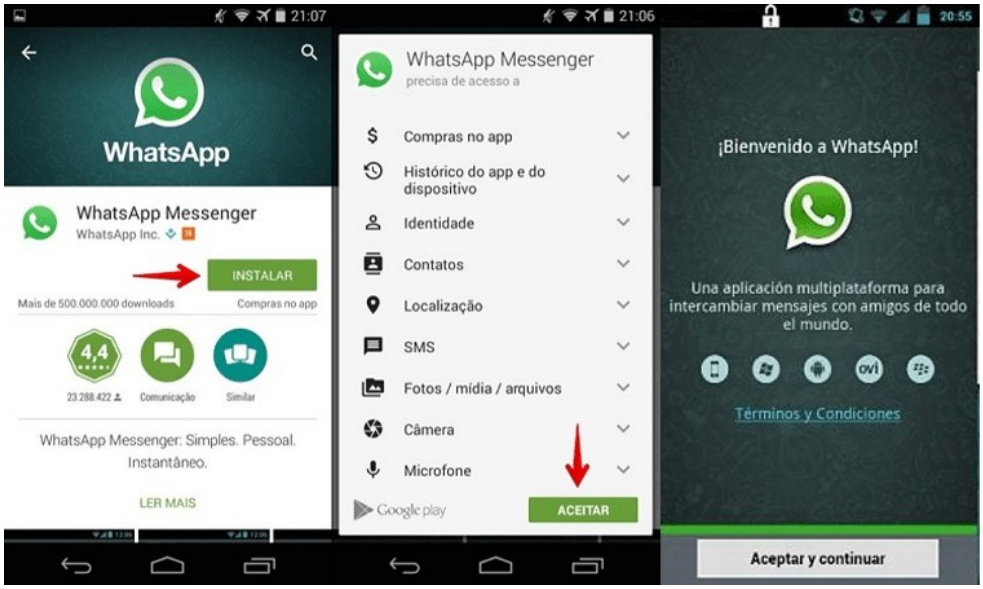
4.1.2 Grans corporacions de la comunicació

No pot ser «Big Data, Big Brother»[16]

El 14 d'abril de 2019, a TV3 feien el programa de Jordi Basté «No pot ser» amb el títol: Big Data, Big Brother, i estava dedicat als sistemes de control i les xarxes socials, dos elements associats. Aquesta vegada Basté viatja al cor de Palo Alto, a Califòrnia, per visitar l'enginyer català Elies Campo, desenvolupador de negoci de Telegram (una de les xarxes socials importants en nombre d'usuaris). Elies Campo, va abandonar WhatsApp quan Facebook la va comprar, per les polítiques de poca transparència d'aquesta empresa. També hi apareix la Marta Peirano[17], experta en privacitat i seguretat a internet, ambdós ens alerten de les empreses dedicades a recopilar i vendre dades personals. Basté també ho tracta amb el fundador d'una d'aquestes empreses: David Tomàs, propietari de *Cyberclick*, que ens explica què hi ha darrere de la «publicitat personalitzada» que han generat les nostres dades a la xarxa. A més a més, hi intervé el periodista nord-americà Andrew Keen, autor de «Internet no és la resposta», molt crític amb el negoci de les xarxes socials.

Una de les diverses tècniques que utilitzen aquestes companyies és que si vols accedir a una certa informació o unes aplicacions concretes, estàs obligat a clicar «accepto» i posar les dades que et demanen, perquè si ho rebutges, surts fora sense poder aconseguir anar endavant o accedir a l'aplicació (Figura 9). No cal dir que si acceptes, automàticament facilites les teves dades i localització a l'empresa en qüestió.

Figura 9 (l'aplicació no funciona si no es clica en "acceptar")



Font: https://internetpasoapaso.com/crear-cuenta-whatsapp-messenger/ (24/02/2020)

[16] Tornat a emetre a TV3 el 26 d'abril a les 23:05 hores

[17] *¿Por qué nos vigilan, si no soy nadie?* (2015) https://www.youtube.com/watch?v=NPE7i8wuupk

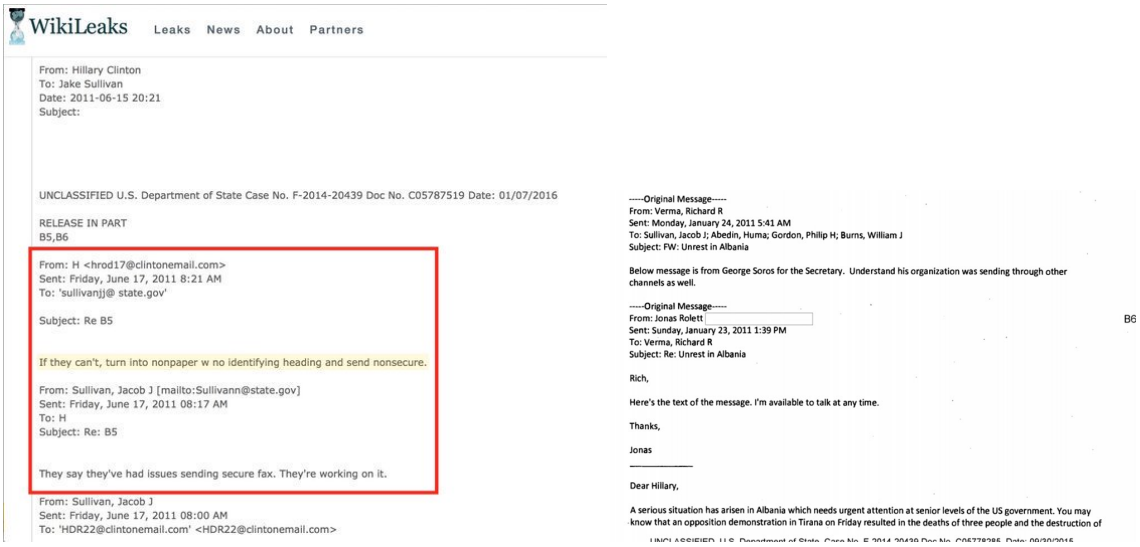
Hi ha diversos arguments i testimonis que demostren que quan ens connectem a internet ja estem delatant que estem fent:

> Por lo general, cuando te conectas a Internet, la solicitud para acceder en cualquier sitio web viaja más o menos directamente de tu ordenador al servidor en el que se aloja el destino final, es decir, el sitio web que intentas visitar. Sin embargo, en todas las paradas de ese camino, tu solicitud anuncia alegremente y con total exactitud de que sitio de la red de Internet procede, y también a cual se dirige, gracias a identificadores llamados 'encabezados de origen y destino' similares en cierto modo a la información del remitente y destinatario de una postal.
>
> (Snowden, 2019: 212

WikiLeaks

Sempre hi ha hagut idealistes com Edward Snowden que han lluitat per denunciar injustícies i donar a conèixer a la població les males pràctiques de les agències de seguretat dels governs que afecten la intimitat de les persones, fins a quin nivell ens controlen, espien i obtenen informació sense la nostra autorització. També es molt conegut tot l'afer de la web WikiLeaks (https://wikileaks.org/) amb Julian Assange[18] al capdavant, per haver "alliberat" molts documents confidencials i amb grans conseqüències per l'administració d'alguns governs. (Holmes, 2018: 159)

Un exemple del tipus de documents que WikiLeaks va publicar per al coneixement de la ciutadania, van ser les *Cartes de Hillary Clinton*. Aquests documents tenien un contingut altament confidencial, i van provocar una gran polèmica des del moment que van sortir a la llum pública, molts dels quals eren correus electrònics de Hillary Clinton, tot i les corresponents protestes, van ser accessibles per a tothom (https://wikileaks.org/clinton-emails/):



[18] Periodista australià i activista d'Internet i que és el director de WikiLeaks (empresa sense afany de lucre), llançada el 2006 i on hi ha des de dissidents xinesos, matemàtics, tècnics d'empreses dels Estats Units, Taiwan, Europa, Austràlia i Sudàfrica. Actualment detingut per la policia britànica i pendent d'extradició als Estats Units per ser jutjat, després d'anys d'exili a l'ambaixada d'Equador a Londres.

> En el ordenador, el FBI encontró unos 650.000 correos, de los que varios miles se enviaron o recibieron desde el servidor privado que tenía Hillary Clinton en su casa y que alojaba la cuenta electrónica privada que usaba como jefa de la diplomacia estadounidense, según dijeron personas conocedoras con la investigación al diario *The Wall Street Journal.*
>
> (Faus, Joan, 2016[19]).

El portal de WikiLeaks revela les tècniques de l'agència i que són pròpies dels hackers i empreses de ciberseguretat. Si partim que tot aparell connectat és susceptible de ser espiat, la CIA ha tingut en el punt de mira qualsevol punt d'accés a internet. L'atac també confirma un dels pitjors temors de «*Internet de les Coses»* com és la capacitat d'utilitzar-lo per a controlar els seus usuaris. Si un televisor "escolta" ordres, també pot "escoltar" converses privades.

Samsung, pionera en aquest camp, inclou una advertència als consumidors, si no volen que la seva veu i el que diguin, quedi enregistrat en els servidors de l'empresa, es millor treure aquesta opció.

A WikiLeaks diuen que el sistema d'escolta i gravació dels televisors de Samsung es va fer en col·laboració amb l'MI5, el servei d'Intel·ligència del Regne Unit. Van crear una falsa sensació d'apagat del mode d'escolta, de manera que tot i suposadament no estava en funcionament, sí que enregistrava el que es parlés a l'habitació on estigués l'aparell, i així enviar-ho als servidors de la CIA. No es limiten només al so, també hi ha la captura d'imatge i el vídeo en aquests televisors. Entre els productes afectats segons WikiLeaks, s'hi troben des de l'iPhone d'Apple als aparells amb sistema *Android, Microsoft*, així com els televisors Samsung. També hi són els *iPads* i els mòdems de connexió a internet.

Les xarxes socials tampoc queden al marge dels hackers de la CIA. WikiLeaks assegura fins i tot que van arribar a prendre el control del Twitter presidencial (Jiménez Cano, 2017).

WikiLeaks sovint actuava com una editorial en quan a la publicació de noticies, però mostrava un especial escepticisme davant el poder estatal. Moltes vegades aquesta organització, s'aliava amb importants diaris del món[20] per fer arribar els documents subministrats per les seves fonts. (Snowden, 2019: 328)

Es pot afirmar sense dubtes que efectivament existeix un control i vigilància permanent sobre els usuaris quan accedeixen a la xarxa. Amb els sofisticats mètodes i aquest gran entramat que s'ha anat teixint durant anys, s'ha creat un sistema ben sòlid que funciona de manera autosuficient amb la intervenció de potents algoritmes. Una de les empreses més populars que està experimentant un

[19] https://elpais.com/internacional/2016/10/31/estados_unidos/1477870911_964962.html?rel=mas (Consulta: 26/11/2019)

[20] *The Guardian, The New York Times, Der Spiegel, Le Monde* i *El País* (Snowden, 2019: 328)

gran creixement entre la població és Amazon, que també utilitza algunes d'aquestes eines per saber que fan els seus clients.

Amazon

El que en podríem dir «control», adopta moltes formes, no sempre es tracte de saber el màxim de dades i moviments dels individus, hi ha altres plataformes com Amazon que utilitzen tècniques diferents i amb l'ús exclusiu de captar i mantenir un sector de clients que comprin els seus productes i es mantinguin fidels. És el cas de *Kindle*, la coneguda aplicació (App[21]) que s'utilitza per poder llegir els llibres d'Amazon en format digital. Tot i que a Europa encara hi ha un consum elevat de llibres en format paper, als Estats Units es calcula que hi ha més gent que llegeix llibres digitals en lloc d'impresos. Amb això juga molt *Kindle* d'Amazon perquè aquest dispositiu pot recopilar dades dels usuaris mentre aquests llegeixen el llibre. Per exemple, el nostre *Kindle* pot supervisar quines parts del llibre llegim ràpid i quines lentament, a quina pàgina vam fer una pausa, i en quina frase abandonem el llibre i ja no el tornem a obrir. (Harari, 2019: 376)

A part del control al qual estem sotmesos des dels governs i les elits del poder a través de les grans empreses i corporacions del món de la comunicació, també hi ha una altre formula de control dins mateix de les empreses, si bé en el món laboral de vegades es reclama un cert nivell d'intimitat, el fet es que l'ús i les dades que generem a través dels dispositius informàtics o de telefonia de l'empresa, no escapem a què quedin enregistrats en els servidors interns i els puguin utilitzar amb la finalitat que vulguin:

> Cada vez son más frecuentes otras formas de control de los trabajadores, como monitorizar todas las acciones que realicen los empleados con los ordenadores y teléfonos inteligentes aportados por la empresa (…) desde las direcciones de las páginas visitadas en Internet hasta el registro de cada pulsación de teclas, o comprobar si el ordenador se utiliza para fines privados, como participar en las redes sociales.
>
> (Holmes, 2017: 29)

Hi ha plataformes que tenen molta difusió com podria ser el cas de Youtube. En els darrers anys s'ha creat un hàbit relacionat amb l'oci per consultar diversos tipus de contingut audiovisual entre la població. Canals dels anomenats *Youtubers* creixen cada vegada més arribant alguns d'ells a tenir centenars de milers de seguidors, això fa que des d'aquesta empresa, també es faci un ús del control que de vegades a causa de les pressions, pot arribar a perjudicar qui només vol transmetre una informació amb caràcter divulgatiu.

Youtube

Hi ha casos on es veu quines intencions i maneres de controlar que es fa o es diu a les xarxes i quan els convé. Arriben a bellugar els fils per fer callar a qui no els interessa, una nova manera de control. Un cas que va sortir als mitjans va ser el de

[21] https://es.wikipedia.org/wiki/APP

Josep Pàmies, activista i fundador de la *Dolça Revolució* -conegut fa uns anys com el pagès de l'estèvia-. Com a conseqüència d'algunes conferències en les que es qüestionava el paper de les farmacèutiques en la nostra salut -tot pel negoci que representen els medicaments- proposava alternatives naturals, però a causa de les pressions d'aquestes elits de poder, van fer que fins i tot "bloquegessin" el canal de Youtube on la *Dolça Revolució*[22] feia difusió d'aquestes medicines i teràpies naturals:

> Tots sabem que l'ús d'una gran plataforma de comunicació com Youtube, aparentment gratuïta, acabarà tenint un cost que pot ser molt alt: el control absolut de tots els seus moviments per a l'usuari final, i per a les empreses, entitats, divulgadors, ... que fem ús d'ells, la restricció a la llibertat d'expressió.
> (La Dolça Revolució: http://dolcarevolucio.cat/language/ca/portada-2/)

Altres mitjans, també han passat per aquesta mateixa situació, és el cas de Mindalia TV que com un canal de difusió sense ànim de lucre i ONG, es dedicava a tractar diversos temes relacionats amb les "teràpies alternatives", però les conseqüències per parlar del «covid19» va fer que Youtube els tanqués el canal i confisqués els seus milers de vídeos: https://youtu.be/U3np8XIQ190 (10/04/2020). El mateix es pot dir d'un altre canal anomenat La Caja de Pandora, el qual es dedicava a la difusió d'espais de diversos àmbits, entre ells, també les medicines alternatives, això va provocar el tancament del canal per part de Youtube: https://youtu.be/fX7Mi4lEHtY (10/04/2020).
Amb actuacions d'aquest tipus es posa de manifest que efectivament hi ha un control a la xarxa i que les grans empreses quan reben pressions perquè no es publiquin uns temes determinats, o que els continguts poden perjudicar la «seva imatge i les seves polítiques econòmiques» decideixen tancar canals i les pàgines web sense donar explicacions.

El tema de la pandèmia global del coronavirus ha estat present com a font de consulta i informació d'una manera espectacular. A través dels mitjans de comunicació s'ha pogut conèixer que hi ha hagut un increment de control a xarxes per part d'empreses com Google fent seguiment de diverses dades relatives al confinament de cada país.[23]
Però no solament es pot parlar de Google, en aquest cas també hi estan implicats els governs[24] que aprofitant la pandèmia com excusa, obertament van informar que es va posar en marxa un programa de seguiment i monitorització dels moviments dels usuaris de telèfons mòbils. Un fet més que confirma mecanismes de control social a través de la geolocalització, tot i que asseguren que les dades seran anònimes, una vegada més es fa evident que són mesures que es van imposant sobre la població. La informació i dades obtingudes, estaran a la seva disposició i quedant emmagatzemades en els seus servidors per sempre.

---

[22] Censura intolerable a Youtube: https://youtu.be/thzTjeecr1A
[23] Planas Bou, Carles (2020): https://www.elperiodico.cat/ca/societat/20200403/google-estadisticas-mobilitat-confinament-131-paises-7915896 (Consultat: 03/04/2020) / Sesé, Gerard (2020) https://www.larepublica.cat/noticies/politica/internacional/les-inquietants-dades-que-ofereix-lestat-sobre-els-desplacaments-de-les-persones-geolocalitzant-dels-mobils/ (Consultat: 18/04/2020)

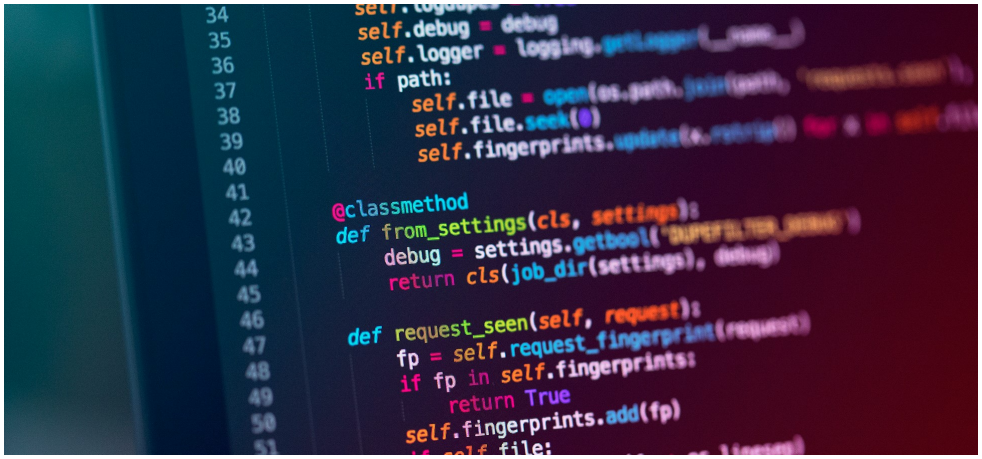
[24] Nadal, Albert / Garcia, Auri (2020): https://www.ara.cat/societat/coronaivirus-covid-19-mobilitat-estudi_0_2433356827.html (Consultat: 16/04/2020)

4.2 Algoritmes

¿Què és un Algoritme? Es poden trobar moltes definicions, però actualment, es podria dir sense cap dubte que «algoritme» és el concepte tecnològic més important a les xarxes socials:

> Un algoritmo es un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones. Un algoritmo no es un cálculo concreto, sino el método que se sigue cuando se hace el cálculo.
>
> (Harari, 2019: 100)

Per exemple, una recepta de cuina és un algoritme perquè segueix un ordre en el que intervenen els ingredients, quan s'han de posar i el temps de cocció. El procés per arribar a un resultat final que és el plat acabat de cuinar.
Amb el llenguatge de programació, les grans empreses tecnològiques utilitzen algoritmes que contenen milers o cents de milers de línies de codis:



Exemple d'algoritme. Font: https://planetachatbot.com/algoritmo-la-palabra-magica-b58f8b1d20cf (Consultat: 20/01/2020)

Els algoritmes estableixen correlacions entre diverses dades d'una mateixa persona i entre els de persones diferents. Aquestes correlacions constitueixen, de fet, teories sobre la naturalesa de cada individu que es mesuren i classifiquen contínuament i van millorant amb el temps a través d'un procés de retroalimentació. (Lanier, 2018: 47)

L'algoritme de Google és el que decideix la forma de posicionar les pàgines en una cerca: que surt primer, segon, o a la pàgina següent. Aquest algoritme canvia unes 500 vegades a l'any[25] i resulta molt difícil seguir-li la pista.

Un fet molt important i decisiu és el que es va produir el 4 de desembre de 2009 perquè a partir d'aquesta data és quan va començar l'*era de la personalització* (Pariser, 2017: 11-13). A partir d'aquí Google utilitzaria fins a 57 indicadors: des del

[25] https://www.forbes.com.mx/con-que-frecuencia-google-cambia-su-algoritmo/

lloc, el navegador i el que s'hagués buscat, per a conjecturar qui ets i quina classe de pàgines web t'agraden. Ara, cada usuari obté un resultat de cerca que pot arribar a ser totalment diferent d'un altre en funció dels enllaços amb altres pàgines que hagi estat buscant i que l'algoritme de Google suggereix que és millor. En altres paraules, ja no existeix un Google estàndard.

Un exemple clar del funcionament dels algoritmes està en una de les empreses paradigmàtiques del sector com és Netflix. Avui dia ja no es va tant al cinema com abans, i a part, les series de televisió ja han passat a la història, per tant, aquí es posa evident com aquestes plataformes tenen cada vegada més acceptació entre la població.

Netflix

Aquesta popular empresa està creixent de manera exponencial i és una de les preferides dels usuaris per visionar pel·lícules i sèries. Netflix funciona a través d'un algoritme anomenat CineMatch. Pariser explica que si un usuari ha vist la primera pel·lícula de *El senyor dels anells*, per exemple, Netflix pot buscar quines altres pel·lícules han vist els espectadors de *El senyor dels anells*, si molts han vist *La guerra de las galàxies*, és molt probable que aquest usuari la vulgui veure perquè el sistema li oferirà. Aquesta tècnica es diu Knn (K-nearest-neighbor), i amb aquesta, l'algoritme CineMatch ha estat decisiu en determinar quines pel·lícules volia veure la gent en funció de les pel·lícules que havien vist els altres usuaris i quina qualificació (en estrelles) li havien posat a les pel·lícules vistes. (Pariser, 2017:132)

Totes les companyies tenen els seus algoritmes registrats i patentats. En el cas de Facebook, té el nom de EdgeRank i es tracte de l'algoritme que carrega la pàgina predeterminada de la web, la secció de noticies. EdgeRank classifica qualsevol interacció amb la pàgina.

En els darrers anys s'estan desenvolupant algoritmes molt superiors que utilitzen una potència de computació sense precedents i bases de dades gegantines. Els algoritmes de Google i Facebook no només saben exactament com ens sentim, si no també un milió de dades més sobre nosaltres mateixos que ni tant sols sospitem. (Harari, 2019: 425-426)
S'ha vist com la clau del funcionament del sistema són els algoritmes que de manera molt sofisticada creen unes rutines i conjunts de procediments per arribar allà on calgui.

Una altre eina desenvolupada i no menys important, és el *big data*, que s'erigeix com la manera en la qual es creen i emmagatzemen tota classe de dades que anem generant a la xarxa i que no paren de créixer.

4.3 Big data

Big data o dades massives[26], «és el nom que reben els conjunts de dades, els procediments i les aplicacions informàtiques, que, pel seu volum, la seva naturalesa

[26] https://ca.wikipedia.org/wiki/Dades_massives

diversa i la velocitat a què han de ser processades, ultrapassen la capacitat dels sistemes informàtics habituals. Aquest processament de dades massives s'utilitza per a detectar patrons dins seu, podent fer així prediccions vàlides per a la presa de decisions».

Segons Harari, l'aparició del dataisme diu: «Como toda religión tiene sus mandamientos prácticos. El primero y principal: un dataísta debe maximizar el flujo de datos conectandose cada vez a más medios, y produciendo y consumiendo cada vez más información. Como otras religiones de éxito, el dataismo también es misionero. Su segundo mandamiento es conectarlo al sistema, incluidos los herejes que no quieren ser conectados». Afirma que al final tot acabarà connectat, no només les persones, també «totes les coses», des dels cotxes als electrodomèstics fins arribar als animals i als arbres. «De ahí que el dataismo sostenga que la libertad de información es el mayor de todos los bienes». (Harari, 2018:415)

La sanitat cada vegada es troba més informatitzada i és una àrea que afecta a un percentatge molt gran i creixent de la població mundial. Els expedients mèdics electrònics es van convertint en la norma en els hospitals i a les consultes. Avui dia, per exemple, si ens fem una anàlisi de sang, o ens atenen en un servei d'urgències d'un hospital, ens faciliten una contrasenya amb la qual poder accedir al nostre historial i imprimir o consultar els resultats. No cal dir, que aquesta informació, ja queda allà i cada vegada que vagis al metge va creixent i actualitzant les teves dades.

La recopilació de dades personals està en alça (ho diu la mateixa Cathy O'Neal en el seu llibre *Armas de destrucción matemática*) però que tot va dirigit a proporcionar una millor assistència sanitària. Ara es possible seguir a distància la salut d'un pacient a temps real enregistrant dades de la pressió sanguínia, el ritme del cor i la temperatura, el que es pot entendre com una manera de reduir despeses i millorar la qualitat de vida. Hi ha dispositius de «monitorització» remota que cada vegada són més sofisticats.

Harari també coincideix en aquest punt, relacionant el capitalisme amb el flux de dades i el dataisme. Les dades ho mouen tot i estan a tot arreu.

> De la misma manera que los capitalistas de libre mercado creen en la mano invisible del mercado, los dataísta creen en la mano invisible del flujo de datos.
>
> (Harari, 2018: 419)

Aquí és on sovint es diu que l'aplicació del big data és de fet una realitat i on més profit se'n traurà en el futur, no se sap si amb això es pensa de manera honesta en el benefici del pacient, o en tot cas el fons de la qüestió es saber-ho tot de cada persona i en certa manera, una forma més de control.

Hi ha empreses que ofereixen incentius als treballadors perquè utilitzin dispositius portàtils per a mesurar la forma física amb la finalitat d'aconseguir certs objectius, com baixar de pes, etc. A canvi de rebre l'aparell, l'empleat accepta compartir les dades amb la companyia.

Per una altra banda el big data està provocant una gran discriminació en el món laboral perquè les grans empreses que recullen dades van creant els perfils de la població on s'hi reflecteix tot l'historial.

En casos que alguna persona hagi tingut algun problema mèdic que hagi provocat el fet de deixar uns estudis o una feina en una empresa, quedarà marcat en el seu historial, i posteriorment, si un dia fa una sol·licitud de treball es veurà perjudicat per aquest fet. (O'Neal, 2017: 131-135)

Actualment es gairebé impossible participar en qualsevol activitat en el decurs de la qual no quedin registres electrònics de dades personals.

> Avui dia es registra cada clic que fem, cada paraula que introduïm en el buscador, tot a la xarxa és observat i vigilat. La nostra vida es reprodueix en la xarxa digital. Ara també vigilen les coses que utilitzem diàriament, és la culminació de la societat de control digital. Vivim en la època del Big Data, i aquest no oblida res.
>
> (Byung-Chul Han, 2014: 93-94)

Les caixes de pagament dels supermercats i centres comercials a través de les targetes de fidelització del clients, guarden dades del que comprem. Quan adquirim bitllets d'avió, les línies aèries també tenen la informació sobre els nostres plans de viatge. Els bancs emmagatzemen les nostres dades financeres i fiscals. Les dades massives que s'utilitzen àmpliament en el comerç i la medicina, troben aplicacions en dret, sociologia, publicitat, sanitat i en totes les àrees de les ciències. Aquestes dades estan en totes les seves formes.

Diverses tècniques i algoritmes, desenvolupats per especialistes en estadística i informàtica, busquen patrons en les dades. La clau de l'èxit en anàlisi de dades massives radica en determinar quins patrons són els rellevants.

> Todos y cada uno de los clics que se efectúan durante la navegación por la Red se registran y se utilizan para producir publicidad dirigida.
>
> (Holmes, 2017:130)

Aquestes dades sobre els usuaris, s'envien a les xarxes publicitàries de tercers i s'emmagatzemen en l'ordinador local en forma de *cookie* (galeta) que té la funció de fixar la localització i punt d'accés de l'usuari. Al clicar en altres llocs d'internet atesos per la mateixa xarxa publicitària apareixen en la pantalla anuncis de productes relacionats amb els clics previs.

Una definició que s'utilitza sovint relacionada amb les dades i al mateix temps amb la seguretat, és el del «núvol» o espai virtual. Abans de l'era digital la gent guardava fotos en àlbums i els negatius realment eren com la còpia de seguretat. Però en els darrers anys tot el que està relacionat amb la seguretat de dades massives ha canviat.

Ara, la majoria de la gent, a part de guardar arxius en el seu propi ordinador, siguin documents, fotos, vídeos o arxius multimèdia, se sol dir que per qüestions de

seguretat personal, en cas que els nostre ordinador s'espatllés, o entres un virus que impedís accedir a les nostres dades, hi ha el costum força estès de penjar còpies d'aquests arxius a l'espai virtual (Google Drive o OneDrive) que algunes d'aquestes companyies han creat per aquesta finalitat i per donar serveis als seus usuaris enregistrats. A part també ens va bé perquè aquests tipus d'arxiu ocupen molt espai, i d'aquesta manera alliberem la memòria dels nostres ordinadors. Al mateix temps el núvol te l'avantatge que s'hi pot accedir des de qualsevol altre ordinador i lloc del món simplement entrant amb la nostra contrasenya. Potser el que molta gent no sap, és que totes les dades que posem al núvol, ja queden emmagatzemades allà per sempre, encara que les hàgim eliminat, ja estan en els servidors d'aquestes empreses, i a més, no podem reclamar res perquè realment els propietaris del núvol no som nosaltres els usuaris si no la pròpia companyia qui a més es reserva el dret d'eliminar els nostres arxius pel motiu que sigui, si li convé. (Holmes, 2018) Altres autors també coincideixen en aquest aspecte (Lanier, 2018; Pariser, 2017).

Acxiom

És l'empresa privada de dades més important del món, amb seu a Arkansas (Estats Units) té més de 2.000 empleats. Aquesta empresa comercialitza dades personals d'aproximadament 300 milions de ciutadans dels Estats Units, pràcticament la majoria, i a més són agrupats en 70 categories diferents. Els arriben a oferir en un catàleg com mercaderia. (Byun-Chul Han, 2014: 99) Acxiom disposa de tanta informació que fins i tot el FBI de vegades recorre a ells per demanar informació d'alguns individus.

Acxiom és l'empresa del big data, de fet el seu eslògan diu: «Les ofrecemos una visión de 360º sobre sus clientes». (Íbid, 2014: 86)

Està clar que el segle XXI ha estat determinant en quan a les polítiques en l'aplicació dels dispositius connectats a la xarxa. Les nostres dades personals són probablement el recurs més valuós que la majoria dels humans encara pot oferir, i els estem cedint als gegants tecnològics a canvi de serveis de correu electrònic (com el Gmail), i altres tipus de jocs per entretenir-se. (Harari, 2019)

Si els *algoritmes* creen el procés en el qual funcionen totes les operacions a la xarxa, el *big data* recull, emmagatzema i gestiona les dades que van creixent, els *bots* són el complement que es posa al nostre servei o ens atén per teòricament donar-nos un servei o resposta a les nostres demandes.

4.4 Bots

Com a «bots» es poden entendre diverses coses, però una definició clara seria «les persones falses». Aquestes persones falses existeixen en grans quantitats i marquen el to. El bots, són també IA (Intel·ligències Artificials), ressenyes falses, amics falsos, seguidors falsos, publicacions falses, perfils falsos automatitzats, es pot dir que es tracte de tota una col·lecció d'entitats «fantasmagòriques» (Lanier, 2018:54).

Els bots[27] són elements fonamentals en el camp de les aplicacions que tenen a veure amb les tecnologies a la xarxa. Bot, és una abreviatura paraula robot (que vol dir esclau). En aquest cas, es tracte d'un software (programa informàtic) que serveix per a comunicar-se amb l'usuari, imitant el comportament humà. En certa manera, es podria dir que els bots estan començant a dominar el món. De vegades podem pensar que darrera una aplicació informàtica o de mòbil (app), hi ha persones gestionant l'activitat, quan realment no és així. La majoria són programes informàtics «autosuficients» que contenen els paràmetres necessaris per donar resposta a l'usuari. També són coneguts per la recent aparició al mercat, dels bots «domèstics» pensats per a les llars als quals se li poden fer consultes gràcies a un altaveu que porten incorporat. Al 2010 l'empresa Apple va llençar al mercat un bot amb el nom de *Siri*, que poc després va començar a instal·lar en els seus iPhon. Dos anys més tard Google va treure el seu assistent anomenat *Now*, i al 2014 Microsoft tenia el seu, amb el nom de *Cortana*. Després el *Bixby* de Samsung, i *Alexa* d'Amazon. A tots aquests bots se'ls hi pot preguntar qualsevol cosa en veu alta o demanar una gestió, i tot seguit, donen la resposta a l'usuari. Tota la informació i dades, queden enregistrades als servidors de les corresponents empreses.

Un programa bot en el núvol d'Amazon supervisa el preu dels llibres que un autor ven en qualsevol lloc del món, per assegurar-se automàticament que Amazon sempre ofereix el preu més baix. (*Íbid*, 2018: 96-97)

Actualment es pot dir que totes les empreses també tenen un «assistent» que atén les nostres consultes i respon les preguntes que li fem. Senzillament és un bot. Aquest dispositiu es connecta a internet i utilitzant la xarxa facilita la informació que se li demana. Sembla una joguina, practica i divertida, i aparentment útil, ningú ho negarà, oi? Però el que no es diu, es que tot el que li preguntem i volem saber, queda enregistrat als servidors de la companyia en qüestió, i al dir tot, també és la veu de l'usuari, que una vegada emmagatzemada, la poden utilitzar pel que vulguin.

Els bots que actuen com assistents domèstics estan disponibles en totes les empreses de comunicació i telefonia (Harari, 2019: 374-376) des de Cortana de Microsoft, Alexa de Google, etc. i operatius en moltes llars, cosa que els permet espiar a famílies senceres.

Segons unes informacions publicades al diari The New York Times, a començament de l'any 2018 el preu de les persones falses a Twitter era de 225 dòlars pels primers 25.000 seguidors falsos. Realment es preocupant que hi hagi empreses podríem dir també falses, que es dediquen a això. El diari The Times va descobrir fins i tot que un complex servei de bots, utilitzava una adreça falsa. Veient aquest procediment es pot arribar a la conclusió que molts llocs web si no fos pels bots o persones falses, no existirien. (Lanier, 2018: 76)

[27] https://www.revistagq.com/noticias/tecnologia/articulos/que-son-exactamente-los-bots-y-como-funcionan/25633

5. Conclusions

Els diversos autors consultats, com a experts i crítics que són, a través de les seves obres i treballs d'investigació, coincideixen en molts dels punts abordats en aquest projecte d'investigació. Després d'analitzar les fonts d'informació consultades, es pot parlar de diversos efectes en quan a l'ús de les TIC en la població dels quals destaquen alguns com:

- Perdre la privacitat posant els esdeveniments de les nostres vides a les mans d'aquestes empreses, la cronologia del dia a dia. Saben coses que no confiaríem ni als nostres amics.
- Configuració del perfil de cada persona on hi ha totes les nostres dades, que s'han extret com a conseqüència de les consultes i recerques que hem fet a la xarxa (professional, oci, salut, etc.) com diu Byung-Chul Han (2014: 93-96) «El Registro Total de la Vida».
- Destrucció de la comunicació humana.
- Influenciar i/o manipular en les nostres decisions.
- Crear addicció estimulant amb el sistema de «gratificacions» encoratjant a la participació en les xarxes socials fent aportacions de ressenyes en llocs com Google Maps.
- Canviar els nostres hàbits de consum. Els individus són el producte de les xarxes socials, no el client. Monetització. Venen les nostres dades a tercers per interessos econòmics.

La participació habitual en les xarxes socials canvia la manera de comunicació donant l'aparença que això és un joc.

> El veredicte general de la societat positiva es diu "m'agrada". Es significatiu que Facebook es negués conseqüentment a introduir un botó de "no m'agrada". La societat positiva evita tota modalitat de joc de la negativitat, perquè aquesta atura la comunicació. El seu valor es mesura només en la quantitat i la velocitat de l'intercanvi d'informació.
>
> (Byung-Chul Han, 2014:20)

Abandonar les xarxes socials per complet és l'única opció per provocar canvis. Si no es fa, no s'està creant l'espai dins del qual Silicon Valley pot fer alguna cosa per a millorar. De totes formes quan una aplicació comença a funcionar, tothom hi queda atrapat. Es difícil deixar una determinada xarxa social i començar a utilitzar-ne una de diferent, perquè tothom que coneixem ja està en la primera. (Lanier, 2018: 35-37)

Com diu el mateix Eli Pariser (2017) internet va néixer per a facilitar el flux d'idees i informació, s'està tancant sobre ell mateix sota la pressió del comerç i la monetització. Però no és massa tard per a corregir el rumb, Pariser exposa una nova visió que exploti els beneficis de la tecnologia sense caure en els pitjors efectes per a aconseguir que internet assoleixi el seu potencial transformador.

Jaron Lanier (2018) coincideix també en que internet i el seu ús no ha de ser dolent, l'únic problema radica en els sistemes de control que imposen les grans empreses que dominen les xarxes socials i amb les quals cal anar en compte per tal de garantir al màxim la nostra privacitat.

Davant el que es mostra com un risc i una forma legal de vulneració de les nostres dades i l'ús que se'n fa d'elles, ens podem plantejar si cal fugir dels sistema, donar-se de baixa de tot i no utilitzar els dispositius connectats a la xarxa perquè no segueixin especulant amb les nostres vides. Lanier (2018) fa la hipotètica pregunta sobre com es pot sobreviure sense les xarxes socials, però ell mateix obre la porta a treure'n un ús profitós sense haver de renunciar a internet. Avui dia internet s'ha arribat a fer pràcticament imprescindible, així que no l'hem de rebutjar, utilitzem-ho amb el que ens faci falta perquè internet en sí, no és el problema. No cal renunciar als nostres amics, se'ls hi pot escriure un correu electrònic en lloc de contactar a través de les xarxes socials, però utilitzant proveïdors que no llegeixen els missatges (com és el cas del Gmail). Es poden seguir llegint les noticies en línia directament dels llocs web, no dels canals personalitzats ni des de les xarxes socials. També es poden seguir veient vídeos a Youtube sense haver de tenir un compte a Google. I en resum, es recomanable abandonar tots aquests llocs com WhatsApp o Instagram que la majoria de la gent utilitza com a cercle d'amistats, perquè no deixen de ser Facebook, de qui són propietat i per tant, també recopilen les nostres dades i ens espien. (Lanier, 2018: 168)

Tots estem atrapats dintre del sistema. Com a mínim el que si podem fer és anar en compte perquè no creixin més les nostres les dades i mantenir al màxim la nostre privacitat.

Bibliografia:

Byung-Chul Han (2010). *La Societat de la transparència*. Herder Editorial. Barcelona

Byung-Chul Han (2014). *Psicopolítica*. Herder Editorial. Barcelona

Giant, Nikki (2016). *Ciber-seguridad para la I-Generación. Usos y riesgos de las redes sociales y sus aplicaciones*. Narcea, S.A. de Ediciones. Madrid.

Harari, Yuval Noah (2018). *Homo Deus: Breve historia del mañana*. Debate. Barcelona.

Harari, Yuval Noah (2019). *21 Lecciones para el siglo XXI*. Barcelona: Debate.

Holmes, Dawn E. (2018). *BIG DATA, una breve introducción*. Antoni Bosch editor, S.A.U. Barcelona

Lanier, Jaron (2014). *¿Quién controla el futuro?.* Editorial Debate. Barcelona

Lanier, Jaron. (2018) *Diez razones para borrar tus redes sociales de inmediato*. Editorial Debate. Barcelona.

Lloyd, Tanya (2017). *Ojos y espias. Cómo te controlan y porque debes saberlo*. Ediciones Siruela, S.A. Madrid.

O'Neil, C. (2017). *Armas de destrucción matemática: cómo el big data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing.

Pariser, E. (2017). *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos*. Barcelona: Taurus.

Snowden, Edward (2019). *Vigilancia permanente*. Editorial Planeta, S.A. Barcelona.

Infografia:

Alphabet: https://ca.wikipedia.org/wiki/Alphabet_Inc. (Consulta: 02/02/2020)

ACXIOM: https://www.acxiom.com/ (Consulta: 11/10/2019)

Algoritme (imatge 14/12/2018): https://planetachatbot.com/algoritmo-la-palabra-magica-b58f8b1d20cf (Consultat: 20/01/2020)

ARPANET: https://ca.wikipedia.org/wiki/ARPANET (26/11/2019)

Cadwalladr, Carole / Graham-Harrison, Emma (publicat 17/03/2018):

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us- election 22/08/2019)

Cambridge Analytica: https://es.wikipedia.org/wiki/Cambridge_Analytica#Esc%C3%A1ndalo_de_Facebook (Consulta: 13/01/2020)

CERN: https://ca.wikipedia.org/wiki/Organitzaci%C3%B3_Europea_per_a_la_Recerca_Nuclear (Consulta: 13/01/2020)

Club Bilderberg: https://es.wikipedia.org/wiki/Grupo_Bilderberg (Consulta: 13/01/2020)

Dades massives (big data): https://ca.wikipedia.org/wiki/Dades_massives (Consulta: 13/01/2020)

DNS: https://www.atinternet.com/es/glosario/dns/ (consulta: 04/02/2020)

EBay: https://ca.wikipedia.org/wiki/EBay (consulta: 04/02/2020)

Explore Google Data Center (fragment de vídeo on es mostra una secció dels potent servidors de l'empresa on es emmagatzemen les dades i es fan bilions de recerques): https://youtu.be/avP5d16wEp0?t=40 (consulta: 03/02/2020)

Faus, J. (2016): https://elpais.com/internacional/2016/10/31/estados_unidos/1477870911_964962.html?rel=mas

https://elpais.com/internacional/2016/11/01/estados_unidos/1477959767_837306.html (Consulta: 26/11/2019)

Forbes (Algoritmo): https://www.forbes.com.mx/con-que-frecuencia-google-cambia-su-algoritmo/ (consulta: 25/03/2020)

Galeano, Susana (2020): https://marketing4ecommerce.net/cuales-redes-sociales-con-mas-usuarios-mundo-2019-top/ (Consulta: 21/02/2020)

Haj-Saleh, Alberto (2017). *Qué son exactamente los 'bots' y cómo funcionan*. Revista GQ (Publicada 05/03/2017) https://www.revistagq.com/noticias/tecnologia/articulos/que-son-exactamente-los-bots-y-como-funcionan/25633 (consulta: 04/02/2020)

Històric/ Internet (1971-2015): https://www.marketingdirecto.com/wpcontent/uploads/2015/05/inernetAcademi_Infografia_HistoriaInternet-1.jpg (consulta: 21/01/2020)

HOST: https://ca.wikipedia.org/wiki/Host_(Inform%C3%A0tica) (consulta: 04/02/2020)

How Google Search Works (in 5 minutes): https://www.youtube.com/watch?v=0eKVizvYSUQ (consulta: 04/02/2020)

Instagram: https://ca.wikipedia.org/wiki/Instagram (consulta: 04/02/2020)

Internet: https://marketing4ecommerce.net/usuarios-internet-mundo/ (consulta: 04/02/2020)

Jiménez Cano, R. (2015): "Así espía la CIA en Internet, según Wikileaks"

https://elpais.com/internacional/2017/03/07/estados_unidos/1488902840_337837.html

(Consulta: 26/11/2019)

L'home més perillós d'Amèrica (Dani Ellsberg): https://www.ccma.cat/tv3/Lhome-mes-perillos-dAmerica-a-Grans-documentals-33/noticia-arxiu/493520/ (consultat: 26/11/2019)

Mazo, Estela, S. (2014): https://www.expansion.com/2014/02/19/empresas/tmt/1392849185.html

McAskill, E. (2018) Conversaciones con Snowden y Ellsberg (Traducido por Lucía Balducci): https://www.eldiario.es/theguardian/Conversaciones-Edward-Snowden-Daniel-Ellsberg_0_730727271.html (Consulta: 27/11/2019)

Márquez, W. (2013). BBC_Mundo: https://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm (Consulta: 09/12/2019)

Mente alternativa.com (29/05/2019): https://www.mentealternativa.com/reunion-secreta-club-bilderberg-2019-por-la-supervivencia-del-modelo-parasitario-de-la-banca-liberal/ (Consulta: 13/02/2020)

Nadal, Albert / Garcia, Auri (2020): https://www.ara.cat/societat/coronaivirus-covid-19-mobilitat-estudi_0_2433356827.html (Consultat: 16/04/2020)

Pascual, Juan Antonio (2019) *Computer Hoy*. https://computerhoy.com/noticias/tecnologia/facebook-borra-historial-borrarlo-matrix-4-oficial-otras-noticias-tecnologicas-resumidas-478457 (Consulta: 22/08/2019)

REGLAMENTO DE PROTECCIÓN DE DATOS (UE) 2016 / 679 – Directiva 95/46: https://www.boe.es/doue/2016/119/L00001-00088.pdf (Consulta: 02/02/2019)

Robot: https://www.xatakaciencia.com/robotica/el-origen-de-la-palabra-robot (Consultat.03/12/2019)

Rodriguez, Guillermo (31/07/2011): https://www.vix.com/es/btg/curiosidades/2011/07/31/quien-invento-el-primer-telefono-movil (26/11/2019)

Saiz, Eva (10/06/2013): El País: https://elpais.com/internacional/2013/06/09/actualidad/1370806341_432561.html (Consultat: 20/08/2019)

Sánchez, Álvaro. El País (20/03/2018): https://elpais.com/internacional/2018/03/19/estados_unidos/1521500023_469300.html (Consultat: 20/08/2019)

Sesé, Gerard (2020) https://www.larepublica.cat/noticies/politica/internacional/les-inquietants-dades-que-ofereix-lestat-sobre-els-desplacaments-de-les-persones-geolocalitzant-dels-mobils/ (Consultat: 18/04/2020)

Snowden, Edward: https://ca.wikipedia.org/wiki/Edward_Snowden (Consultat: 20/01/2020)

The Guardian (Mark Zuckerberg): https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook (publicat: 22/05/2016) (Consultat: 22/11/2019)

Tu.Blog.Tecnológico: http://tublogtecnologico.com/las-redes-sociales-mas-utilizadas-segun-la-edad/ (Consultat: 20/02/2020)

VilaWeb-Redacció (2019). (publicat: 20/08/2019) https://www.vilaweb.cat/noticies/pequin-facebook-twitter-protestes-hong-kong/ (Consultat: 20/08/2019)

WhatsApp: https://ca.wikipedia.org/wiki/WhatsApp (Consultat: 22/11/2019)

WhatsApp (instal·lar aplicació): https://internetpasoapaso.com/crear-cuenta-whatsapp-messenger/ (Consultat: 24/02/2020)

Wikipèdia (algoritme); https://culturadigital.blog.gencat.cat/2015/05/04/saps-que-es-un-algoritme-2/ (Consultat: 27/11/2019)

Wikipèdia (algoritme); https://ca.wikipedia.org/wiki/Algorisme (Consultat: 27/11/2019)

Wikipèdia (Historia d'internet); https://es.wikipedia.org/wiki/Historia_de_Internet (Consultat: 26/11/2019

Wikipèdia (primer telèfon mòbil); https://ca.wikipedia.org/wiki/Motorola_DynaTAC (Consultat: 20/10/2019)

Wikipèdia (veïnatge global); https://ca.wikipedia.org/wiki/Ve%C3%AFnatge_universal (Consultat: 27/11/2019)

Wikipèdia (Xarxes socials); https://ca.wikipedia.org/wiki/Xarxa_social (Consultat: 28/11/2019)

Yahoo!: https://ca.wikipedia.org/wiki/Yahoo! (Consultat: 20/08/2019)

Audiovisuals:

Citizenfour [película] (2014). Dirección Laura Poitras. EUA y Alemania: Práxis Films; Participant Media; HBO Films, 2014. Documental sobre Edward Snowden: https://www.youtube.com/watch?v=KQ0DeRg1IhI

Facebookistan [pel·lícula] (2015). Direcció: Jakob Gottschau. Denmarck and Finland: Danish Film Institute [et al.] https://www.youtube.com/watch?v=R7_VuGADn6w

Història de internet (2011) https://www.youtube.com/watch?v=i4RE6dBAjH4 (Consultat. 26/11/2019)

Internet, breve història (2011): https://www.youtube.com/watch?v=i4RE6dBAjH4&t=44s (Consultat: 21/01/2020)

La Caja de Pandora i el tancament del cana a Youtube (2020): https://youtu.be/fX7Mi4lEHtY (Consultat: 10/04/2020)

La Dolça Revolució. Bloqueig de Youtube: Enllaç a la publicació amb el vídeo bloquejat: https://goo.gl/nfnKrj (https://youtu.be/ZVNk3JeuEDE) (https://youtu.be/thzTjeecr1A)

Las claves de internet (2018) ; https://www.youtube.com/watch?v=dkWXJFcuaRo (Simonfilm) (Consultat: 26/11/2019)

Mindalia TV i el tancament del canal a Youtube (2020): https://youtu.be/U3np8XIQ190 (Consultat: 10/04/2020)

Planas Bou, Carles (2020): https://www.elperiodico.cat/ca/societat/20200403/google-estadisticas-mobilitat-confinament-131-paises-7915896 (Consultat: 03/04/2020)

Peirano, Marta (2015) *¿Por qué nos vigilan, si no soy nadie?* (Vídeo) https://www.youtube.com/watch?v=NPE7i8wuupk

TV3 (2019).*No pot ser*. (emissió: 14-04-2019):

https://www.ccma.cat/tv3/alacarta/no-pot-ser/big-data-big-brother/video/5836380/ (Consulta: 14/04/2019)

Films:

La Red Social (2010): https://www.youtube.com/watch?v=XHmtg0bWQr0&t=39s (Mark Zuckerberg i Facebook)

Snowden (2016): https://www.youtube.com/watch?v=kGbQt8D2eA0 (El relat de l'Edward Snowden)

Secretos de Estado (2019). https://www.youtube.com/watch?v=HWdyLiyYJw4 (un cas basat en fets reals sobre l'agència d'espionatge britànica GCHQ)